Data Protection
Commissioner
An Coimisinéir Cosanta Sonraí

Annual Report



03

To seek to make a difference in generating cultural change in organisations regarding respect for data protection and privacy and in generating awareness amongst the public about their rights

Data Protection at a Glance

What is data protection?

It is the safeguarding of the privacy rights of individuals in relation to the processing of personal data. The Data Protection Acts 1988 and 2003 confer rights on individuals as well as placing responsibilities on those persons processing personal data.

Individuals have a number of legal rights under data protection law. You can…

- expect fair treatment from organisations in the way they obtain, keep, use and share your information;
- demand to see a copy of all information about you kept by the organisation;
- stop an organisation from using your details for direct marketing;
- demand that inaccurate information about you be corrected;
- demand that any information about you be deleted, if the organisation has no valid reason to hold it;
- complain to the Data Protection Commissioner if you feel your data protection rights are being infringed;
- sue an organisation through the courts if you have suffered damage through the mishandling of information about you.

To comply with their data protection obligations data controllers must…

- obtain and process the information fairly;
- keep it only for one or more specified, explicit and lawful purposes;
- use and disclose it only in ways compatible with these purposes;
- keep it safe and secure;
- keep it accurate, complete and up-to-date;
- ensure that it is adequate, relevant and not excessive;
- retain it no longer than is necessary for the specified purpose or purposes;
- give a copy of his/her personal data to any individual, on request.

Data Protection
Commissioner
An Coimisinéir Cosanta Sonraí

Fifteenth Annual Report

of the

Data Protection Commissioner

2003

Presented to each House of the Oireachtas pursuant to section 14 of the Data Protection Acts, 1988 & 2003

PRN. 2284

Contents

The Office's objective is to seek to make a difference in generating cultural change in organisations regarding respect for data protection and privacy and in generating awareness amongst the public about their rights.

Foreword

Joe Meade
Data Protection Commissioner

Practical Data Protection which takes on board the concerns of Government and Business while respecting the fundamental rights of people is the guiding principle of my Office.

I am pleased to present my fourth Annual Report - it being the fifteenth Annual Report since the Office was established in 1989 - in relation to the work of the Office of the Data Protection Commissioner. It details the activities of my Office during 2003.

Data protection and modern times

Overall, I am responsible for supervising the Data Protection Acts 1988 and 2003, the body of legislation which creates a framework for processing of data about people, conferring as it does, obligations on organisations and rights for individuals, relating to fair processing of personal data. We are living in a period of rapid technological and social change - every year brings new developments and demands - and the question now, often, is not what is technically feasible but whether a particular development is consistent with what we really want as a society. In this regard, as I review the range of issues that my Office faced in 2003 - in both the public and private sectors - it is important to hold that there is a value to our human right of personal privacy. While there are real challenges for society in the face of terrorism, security, efficient administration and so on, there does not have to be a trade-off against privacy. I believe it appropriate to reiterate once again in my annual Report to the Oireachtas that as Data Protection Commissioner I will be supportive of measures that are demonstrably necessary to protect against crime or terrorism but such measures must be proportionate and have regard to the human right to privacy.

Practical Data Protection which takes on board the concerns of Government and Business while respecting the fundamental rights of people is the guiding principle of my Office. The Office's objective is to seek to make a difference in generating cultural change in organisations regarding respect for data protection and privacy and in generating awareness amongst the public about their rights.

Decentralisation

My Office is one of those selected by the Government in December 2003 to be decentralised to Portarlington. In implementing the Government decision my focus will be to ensure that the work of the Office is not significantly affected while at the same time ensuring that the Government decision is implemented in a properly managed fashion. While this will have a major impact on the Office during the coming years and will be a major challenge nevertheless planning for a successful decentralisation has begun.

Developments in 2003

2003 was the year when data protection in Ireland made significant advances as:

- the EU Data Protection Directive 95/46 was eventually transposed into Irish law and became effective from July 2003. The Office engaged in a major awareness campaign chiefly amongst data controllers to alert them to the new provisions. Ireland is now no longer out of step with Europe.

- the EU Directive on data protection in the electronic communications area was also transposed in November 2003. The more stringent measures to combat 'spam' will hopefully bear fruit during the coming year. However law alone will not fully prevent this 'spam' menace and more concerted action at international level is needed with industry as well playing its role. Appendix 1 refers.
- increased levels of activity arose in all sectors with levels increasing by on average 25%
- privacy audits were begun and will be expanded on in the coming year.
- a more focussed awareness campaign has been of benefit.
- the register of controllers registered with the Office and the Office's strategy statement were put on our website.
- a move to a new Office was effected with minimal disruption of service. This has enabled the staff to work in a far more suitable office environment with consequent productivity gains and the capacity to provide better levels of service to personal callers.

Specific areas of attention during 2003:

The following specific measures arose during 2003:

- judicial review proceedings initiated in January 2003, as outlined in Appendix 1 of my 2002 Report, against the Minister for Justice, Equality and Law Reform were postponed pending the promised initiation of primary legislation to regularise the position regarding the retention of communications traffic data following a public consultation by the Minister. It is to be hoped that this matter will be finalised satisfactorily in 2004.
- prosecutions were initiated against two legal firms who failed to register with my Office. It is regrettable that I was left with no option but to take this action despite previous warnings from me in prior annual reports and the strong messages sent by the Law Society to its members. Other sectors who have not fulfilled their statutory requirements with my Office can expect similar actions in the future
- an enforcement notice was issued in October 2003 requiring the Minister for Communications, Marine and Natural Resources to adhere to data protection legislation regarding the publication of personal details on the Departmental website of those who had made FOI requests. The notice was appealed to the Circuit Court but following subsequent discussions between the Attorney General and myself a proposal was agreed, which if acceptable to the Minister, would resolve the matter to my satisfaction. The Minister accepted this agreement and the court appeal hearing then did not proceed. My only aim was to ensure that a person should be able to exercise his/her legal rights under Freedom of Information legislation without having to forego his/her privacy rights. The agreement reached is outlined in Appendix 2
- I ruled that automated SMS texting of an attractive marketing offer - but with an expensive telephone opt out provision - was against data protection principles as well as being of a misleading nature - case study 5 refers. I appreciate Regtel's action in regard to the premium rate phone line once the matter was brought to its attention. The regulation which transposed into law the EU electronic communications privacy directive in November 2003 has satisfactorily clarified any doubts as to my ruling in this matter and I am grateful to the Minister for Communications, Marine and Natural Resources for strengthening the law in this area
- an inspection was carried out, with satisfactory results, at Eircom to review that access to telephone traffic data by law enforcement agencies was in line with the provisions of the 1983/93 Postal and Telecommunications Services Acts and the Data Protection Acts
- in conjunction with the Department of Health and Children, the College of General Practitioners and my Office, a consultative code of practice for general practitioners was launched. In addition the Gardaí have started work on a code of practice for its members and the public. I welcome these developments as it enables data protection to be tailored to the specific requirements of diverse organisations and I look forward to more organisations devising other codes of practice
- at international level the need to strike a proper balance between privacy rights and the need to

combat terrorism was of major concern. In that regard the Article 29 working group - comprising data protection commissioners of EU member states and the EU Commission - outlined concerns regarding the transfer of passenger data to the USA and other countries. It also produced a working paper in the area of biometrics and is working on a paper on genetic data.

The foregoing indicates that the data protection law is complex and sensitive matters are arising which have to be resolved. However as the legislature has given me independent powers to ensure that peoples' privacy rights are respected it is incumbent on me to carry out those powers in as full a manner as is humanly possible.

Employment vetting

I feel it appropriate to make some observations on the whole area of vetting of personnel for jobs. This is a complex area and if not properly implemented could unintentionally cause serious invasion of personal privacy. I reiterate that data protection law is not a barrier to proper scrutiny checks being carried out in sensitive employment areas and constructive discussions have taken place between my Office and An Garda Síochána. Appendix 3 refers.

Future challenges

Biometrics, genetic testing, DNA profiling, identification, authentication, verification, security, marketing profiling, radio frequency identification (RFID's) and sharing of data are some of the issues that are arising and which will impact on peoples' privacy, if not handled in a proportionate manner. It is necessary for policy makers and decision-makers in the public and private sectors to engage with me and indeed with the general public before decisions are made in these areas as otherwise 'bad law' or 'bad practice' may arise. It will be discovered that while my Office will not be averse to the many good consequences that can flow from these measures I do expect that all angles are reviewed including in particular the effect these measures can have on a person's privacy rights. In this regard, I urge public and private sector bodies alike to carry out Privacy Impact Assessments to confirm the compliance of any new organizational or technological initative with the requirements of the Data Protection Acts. Appendices 4 and 5 refer.

Appreciation

I thank the many people who contacted my Office and brought serious matters to notice. I also thank the majority of data controllers who generally complied fully with the law and by working in a spirit of cooperation with my Office the burdens placed on organisations are minimised. I wish again in my annual report, to express my gratitude to the Minister for Justice, Equality and Law Reform and his officials for their support and the continuing good relations between our Offices.

Resources

Data Protection law is now quite complex. Extra resources have been provided to the Office over the last two years which has enabled it to operate more effectively and deal with complaints and registrations in a satisfactory manner. However the focus has to change for the future to providing more guidance compliance notes, codes of practice and detailed information notes so that data controllers are facilitated overall. Furthermore policy aspects are becoming more a part of our daily work and the complex issues arising are resource intensive. I will therefore keep the resource situation under review - sufficient resources were available during 2003 - as I strive to improve the level of service that my office provides. The establishment of a Partnership Committee during the year contributed significantly to the Office's operations as well as facilitating business planning and performance management development overall.

I am pleased to record my special appreciation to the dedicated office personnel for their hard work, professionalism and providing an independent and fair public service in as efficient and competent manner as is feasible. I also record my appreciation to two legal students - from the USA and Ireland - who as part of their studies spent some time working with my staff. I intend to develop this system further as we all found the experience to be productive.

Joe Meade
Data Protection Commissioner

22 March 2004

Réamhrá

Seosamh O'Mídheach
Coimisinéir Cosanta Sonraí

Tá áthas orm an ceathrú Tuarascáil Bhliantúil de mo chuidse - arb í an cúigiú Tuarascáil Bhliantúil ó bunaíodh an oifig sa bhliain 1989 í - a chur i láthair i ndáil le hobair Oifig an Choimisinéara Cosanta Sonraí. Tugann sé mionsonraí faoi ghníomhaíochtaí m'Oifige i rith 2003.

Cosaint Sonraí i gComhthéacs

Tríd is tríd tá an fhreagracht ormsa maoirseacht a dhéanamh ar na hAchtanna um Chosaint Sonraí 1988 agus 2003, an moll reachtaíochta a chruthaíonn creat chun sonraí faoi dhaoine a phróiseáil, ag tabhairt oibligeáidí d'eagraíochtaí agus cearta do dhaoine aonair i ndáil le próiseáil chothrom ar shonraí pearsanta. Táimid ag maireachtáil i dtréimhse ina bhfuil fás teicneolaíochta agus sóisialta ag tarlú go tapa - bíonn forbairtí agus éilimh nua ann gach bliain - agus go minic is í an cheist a bhíonn anois ann, ní cad is féidir a dhéanamh go teicniúil, ach cibé an bhfuil forbairt áirithe ag teacht lena bhfuil uainn i ndáiríre mar shochaí. Maidir leis sin, de réir mar a dhéanaim athbhreithniú ar an raon saincheisteanna a tháinig os comhair m'Oifige in 2003 - san earnáil phoiblí agus san earnáil phríobháideach araon - tá sé tábhachtach a mhaíomh go bhfuil tairbhe lenár gceart daonna ar phríobháideachas pearsanta. Cé go bhfuil dúshláin iarbhíre ann don tsochaí i gcúrsaí sceimhlitheoireachta, slándála, riaracháin éifeachtaigh agus mar sin de, ní gá go mbeadh air sin cur isteach ar phríobháideachas.

Is é treoirphrionsabal m'Oifige ná go mbeadh Cosaint Sonraí Phraiticiúil ann a ghlacann chuige ábhair imní an Rialtais agus an tSaoil Ghnó agus fós go mbíonn meas ar chearta bunúsacha na ndaoine. Is é cuspóir na hOifige, féachaint le difríocht a dhéanamh chun athrú cultúir a chothú in eagraíochtaí maidir le meas ar chosaint sonraí agus ar phríobháideachas agus chun feasacht a chothú i measc an phobail faoina gcearta.

Dílárú

Tá m'Oifigse ar cheann díobh sin a roghnaigh an Rialtas i mí na Nollag 2003 le dílárú go Cúil an tSúdaire. I bhfeidhmiú chinneadh an Rialtais beidh mise dírithe ar a chinntiú nach ndéanfar difear go suntasach d'obair na hOifige agus ag an am céanna a chinntiú go gcuirfear cinneadh an Rialtais i bhfeidhm ar shlí a bheidh bainistithe go cuí. Cé go mbeidh tionchar mór aige sin ar an Oifig i rith na mblianta beaga amach romhainn agus gur dúshlán mór a bheidh ann, mar sin féin tá tús curtha le pleanáil do dhílárú a n-éireoidh leis.

Forbairtí in 2003

Ba í 2003 an bhliain a ndearna cosaint sonraí dul chun cinn suntasach in Éirinn, nuair a tharla na nithe seo a leanas:

- aistríodh an Treoir um Chosaint Sonraí ón AE 95/46 faoi dheireadh isteach i ndlí na hÉireann agus bhí éifeacht léi ó mhí Iúil 2003. Chuaigh an oifig i mbun feachtais mhóir feasachta go príomha i measc rialaitheoirí sonraí chun iad a chur ar an eolas faoi na forálacha nua. Níl Éire i staid nach bhfuil ag teacht leis an Eoraip ar an gceist seo a thuilleadh.
- aistríodh an Treoir ón AE ar chosaint sonraí sa réimse cumarsáide leictreonaí isteach sa dlí chomh maith i mí na Samhna 2003. Táthar ag súil go mbeidh toradh ar na bearta níos déine chun cur in aghaidh 'turscar' i rith na bliana seo chugainn. Ní chuirfidh dlí ann féin, áfach, cosc leis an mbagairt 'turscair' agus tá gá le gníomh níos comhbheartaithe ag leibhéal idirnáisiúnta agus ról a bheith ag an tionscal chomh maith. Tagraítear dó in Aguisín 1.
- tháinig leibhéil níos mó gníomhaíocht chun cinn sna hearnálacha ar fad agus mhéadaigh na leibhéil 25% ar an meán.
- cuireadh tús le hiniúchtaí príobháideachais agus leathnófar iad sa bhliain atá ag teacht.
- bhain sochar le feachtas feasachta le fócas níos mó.
- cuireadh clár na rialaitheoirí atá cláraithe leis an Oifig seo agus ráiteas straitéise na hOifige ar ár láithreán gréasáin.
- rinneadh an t-aistriú chuig Oifig nua lena laghad cur isteach ar sheirbhís agus a d'fhéadfaí. Chuir seo ar chumas na foirne oibriú i dtimpeallacht oifige a bhí níos oiriúnaí le gnóthachain táirgiúlachta mar thoradh air agus an acmhainn leibhéil seirbhíse níos fearr a chur ar fáil do dhaoine a tháinig i bpearsa.

Réimsí sonracha gnó i rith 2003

Tháinig na bearta sonracha seo chun cinn i rith 2003.

- cuireadh imeachtaí athbhreithnithe breithiúnaigh a tionscnaíodh in Eanáir 2003 in aghaidh an Aire Dlí agus Cirt, Comhionannais agus Athchóirithe Dlí siar ag feitheamh ar reachtaíocht phríomhúil a thionscnamh chun rialú a dhéanamh ar an seasamh i ndáil le sonraí tráchta cumarsáide a choinneáil, tar éis geallúint a tugadh ag comhchomhairle leis an Aire. Táthar ag súil go dtabharfar an ní seo chun críche go sásúil in 2004.
- tionscnaíodh ionchúisimh in aghaidh dhá ghnólacht dlí a mhainnigh clárú le m'Oifig. Is mór an trua nach raibh aon rogha agam ach an gníomh sin a dhéanamh d'ainneoin foláirimh a bheith tugtha roimhe sin agam i dtuarascálacha bliantúla roimhe seo agus na teachtaireachtaí láidre a chuir an Dlí-Chumann chuig a chomhaltaí. Is féidir le hearnálacha eile nach bhfuil a gceanglais reachtúla le m'Oifig comhlíonta acu a bheith ag súil le gníomhartha den sórt céanna amach anseo.
- eisíodh fógra forghníomhaithe i mí Deireadh Fómhair á cheangal ar an Aire Cumarsáide, Mara agus Acmhainní Nádúrtha cloí leis an reachtaíocht chosanta sonraí i dáil le mionsonraí pearsanta a fhoilsiú ar láithreán gréasáin na Roinne faoi na daoine a rinne iarrataí saorála faisnéise. Rinneadh achomharc ar an bhfógra chuig an gCúirt Chuarda ach tar éis cainteanna ina dhiaidh sin idir an tArd-Aighne agus mé féin comhaontaíodh moladh, dá mbeadh glacadh ag an Aire leis, a réiteodh an cheist chun mo shástachta. Ghlac an tAire leis an gcomhaontú seo agus ní dheachthas chun cinn le héisteacht an achomhairc. Is é an aidhm a bhí agamsa ná a chinntiú gur cheart go bhféadfadh duine a chearta nó a cearta dlíthiúla faoin reachtaíocht Saorála Faisnéise a dhéanamh gan a bheith orthu a gcearta príobháideachais a ligean uathu. Tá imlíne ar an gcomhaontú sin in Aguisín 2.
- rialaigh mé go raibh téacs uathoibríoch SMS ar thairisicint tarraingteach margaíochta - ach le foráil rogha diúltaithe le teileafón daor - in aghaidh na bprionsabal cosanta sonraí chomh maith le bheith míthreorach de réir nádúir - tagraíonn cás-staidéar. Tuigim gníomh Regtel maidir le líne teileafóin préimh-ráta a luaithe a tugadh an t-ábhar ar a aird. Tá soiléiriú tugtha go sásúil ag na rialacháin a d'aistigh treoir ón AE ar phríobháideachais cumarsáide leictreonaí isteach sa dlí i mí na Samhna 2003 ar aon amhras maidir le mo rialú san ábhar seo agus táim buíoch den Aire Cumarsáide, Mara agus Acmhainní Nádúrtha as an dlí a neartú sa réimse seo.
- rinneadh iniúchadh, le torthaí sásúla, ó thaobh Eircom chun athbhreithniú a dhéanamh go raibh rochtain ag gníomhaireachtaí forfheidhmithe dlí ar shonraí tráchta teileafóin ag teacht le forálacha na nAchtanna Seirbhísí Poist agus Teileachumaráide 1983/93 agus na nAchtanna Cosanta Sonraí.
- i gcomhar leis an Roinn Sláinte agus Leanaí, Coláiste Dhochtúirí Teaghlaigh na hÉireann agus m'Oifig, seoladh cód comhairleach cleachtais do dhochtúirí teaghlaigh. Chomh maith leis sin, tá na Gardaí tosaithe ag obair ar chód cleachtais dá gcomhaltaí agus don phobal. Fáiltím roimh na forbairtí seo mar gur féidir cosaint sonraí a shainoiriúint chuig riachtanais shainiúla na n-eagraíochtaí éagsúla dá mbarr agus táim ag súil le tuilleadh eagraíochtaí a bheith ag ceapadh cóid chleachtais eile.
- ag leibhéal idirnáisiúnta b'ábhar mór imní a bhí sa ghá atá le cothromaíocht chuí a bheith idir cearta príobháideachais agus an gá atá le sceimhlitheoireacht a chomhrac. Ina leith sin, thug grúpa oibre Airteagal 29 - a bhí comhdhéanta de choimisinéirí cosanta sonraí bhallstáit an AE agus Choimisiún an AE - achoimre ar na hábhair imní a bhain le haistriú sonraí paisinéirí chuig SAM agus tíortha eile. Chuir sé páipéar oibre ar fáil freisin i réimse na bithmhéadrachta agus táthar ag obair ar pháipéar ar shonraí géiniteacha.

Tugann a bhfuil thuas le tuiscint go bhfuil an dlí ar chosaint sonraí casta agus go bhfuil ábhair íogaracha ag teacht chun cinn a chaithfear a réiteach. De bhrí go bhfuil cumhachtaí neamhspleácha tugtha dom ag an reachtaíocht, áfach, lena chinntiú go mbíonn meas ar chearta príobháideachais na ndaoine is ormsa atá an dualgas na cumhachtaí sin a dhéanamh ar shlí chomh hiomlán agus is féidir.

Seiceáil Fostaíochta

Mothaím gur cuí roinnt breathnuithe a dhéanamh ar an réimse iomlán de sheiceáil phearsanra do phostanna. Is réimse casta é seo agus mura gcuirtear i bhfeidhm i gceart é d'fhéadfadh sé cur isteach go mór ar phríobháideachas pearsanta, cé nach mbeadh sé beartaithe sin a dhéanamh. Deirim arís, nach bac é

an dlí cosanta sonraí ar sheiceáil cheart slándála a dhéanamh i réimsí íogaireacha fostaíochta agus bhí comhráite éifeachtacha idir m'Oifig agus An Garda Síochána. Tagraítear dó in Aguisín 3.

Dúshláin Amach Anseo.

Tá bithmhéadracht, tástáil ghéiniteach, próifíliú DNA, sainaithint, fíordheimhniú, fíorú, slándáil, próifíliú margaíochta, sainaithint minicíochta raidió (RFIDanna) agus roinnt sonraí ar chuid de na ceisteanna atá ag teacht chun cinn agus a mbeidh tionchar acu ar phríobháideachas na ndaoine, mura láimhseáiltear iad ar shlí cionmhar. Ní mór do dhéantóirí polasaí agus do dhéantóirí cinntí san earnáil phoiblí agus san earnáil phríobháideach dul i gcomhairle liomsa agus go deimhin leis an bpobal i gcoitinne sula ndéantar cinntí sna réimsí seo nó mura ndéantar sin d'fhéadfadh 'drochdhlí' nó droch-chleachtas' teacht chun cinn. Gheofar amach, cé nach mbeidh m'Oifig in aghaidh go leor de na hiarmhairtí maithe a d'fhéadfadh sreabhadh as na bearta sin, go mbeidh mé ag súil go ndéanfar athbhreithniú ar gach gné de lena n-áirítear an éifeacht a bheidh ag na bearta sin ar chearta príobháideachais na ndaoine. Maidir leis sin, mholfainn do chomhlachtaí na hearnála poiblí agus na hearnála príobháidí araon Meastacháin Tionchair Príobháideachais a dhéanamh lena dheimhniú go mbeidh aon thionscnamh nua eagraíochtúil nó teicniúil ag comhlíonadh ceanglais na nAchtanna Coshanta Sonraí. Tagraítear d'Aguisíní 4 agus 5.

Buíochas

Glacaim buíochas leis an iliomad daoine a rinne teagmháil le m'Oifig agus a thug nithe tromchúiseacha ar aird. Glacaim buíochas freisin leis an móramh de rialaitheoirí sonraí a chomhlíon an dlí go hiomlán tríd is tríd agus trí oibriú i spiorad na comhoibre le m'Oifig tá an t-ualach a cuireadh ar eagraíochtaí laghdaithe. Is mian liom arís i mo thuarascáil bhliantúil mo bhuíochas a léiriú don Aire Dlí agus Cirt, Comhionannais agus Athchóirithe Dlí agus lena oifigigh as an tacaíocht agus an dea-chaidreamh leanúnach idir ár nOifigí.

Acmhainní

Tá an dlí Cosanta Sonraí anois sách casta. Tá acmhainní breise curtha ar fáil anois ag an Oifig le dhá bhliain anuas a chuir ar a cumas oibriú níos éifeachtaí agus déileáil le gearáin agus le clárúcháin ar mhodh sásúil. Caithfidh an fócas athrú, áfach, don todhchaí chun tuilleadh nótaí comhlíonta treorach, cóid chleachtais agus nótaí eolais mionsonraithe a sholáthar ionas go n-éascófar na rialaitheoirí sonraí tríd is tríd. Chomh maith leis sin, tá méadú ag teacht ar ghnéithe polasaí a bheith ina gcuid dár n-obair laethúil agus tá na ceisteanna casta atá ag teacht chun cinn dian ar acmhainní. Dá bhrí sin, coinneoidh mé staid na n-acmhainní faoi athbhreithniú - bhí fáil ar dhóthain acmhainní i rith 2003 - de réir mar a dhéanaim mo dhícheall chun feabhas a chur ar an leibhéal seirbhíse a chuireann m'oifig ar fáil. Chuir bunú Coiste Comhpháirtíochta i rith na bliana go suntasach le hoibríochtaí na hOifige chomh maith le pleanáil ghnó agus forbairt bhainistíochta feidhmíochta a éascú tríd is tríd.

Tá áthas orm mo bhuíochas speisialta do phearsanra tiomanta oifige a chur in iúl as an obair chrua a rinne siad, as a ngairmiúlacht agus as seirbhís phoiblí neamhspleách agus chothrom a sholáthar ar mhodh a bhí chomh héifeachtach agus chomh hinniúil agus a d'fhéadfaí. Cuirim mo bhuíochas in iúl freisin do bheirt mhac léinn dlí - ó SAM agus Éirinn - a chaith roinnt ama ag obair le m'fhoireann mar chuid dá staidéar. Tá sé i gceist agam an córas seo a fhorbairt tuilleadh mar gur mhothaigh muid ar fad gur cleachtas tairbheach a bhí sa gcleachtas sin.

Seosamh O'Mídheach
Coimisinéir Cosanta Sonraí

22 Márta 2004

part one

Activities in 2003

Part One

Activities in 2003

Data Protection Law in Context

The Office of the Data Protection Commissioner has a wide range of responsibilities associated with the supervision of the Data Protection Acts 1988 and 2003. In general terms, data protection places obligations on those holding information about people - data controllers - and gives everyone the right to find out what information is being kept about themselves. This means that my Office carries out two main functions. Firstly, we work to ensure that data controllers in carrying out their obligations operate in accordance with the data protection principles. Central to our responsibilities also is the development of awareness among members of the public of their rights, in particular their right to ask for and receive a copy of their own personal data, whether on computer or in a paper file.

My Office is also responsible for overseeing the data protection aspects of the Electronic Communications Regulations 2003 (S.I. No. 535 of 2003), which give effect to EU Directive 2002/58/EC. As the Data Protection (Amendment) Act 2003 also transposed the EC Data Protection Directive (95/46/EC) into our domestic law, my Office therefore plays a significant role in contributing to the development of harmonised approaches to data protection throughout the EU.

Increasingly, public and private sector bodies are recognising that the processing of personal data is central to their work and the services that they provide. Privacy in relation to personal data is a human right but people also need to give their information to organisations all of the time in transactions for goods and services. Data Protection Law by providing a framework for the use of personal data can both reassure people that their data will only be used within their expectations while at the same time allowing organisations to utilise modern technologies for commercial and practical advantage. This is crucial for the on-going and future success of eGovernment and eCommerce initiatives. My Office is regularly consulted by organisations for advice about the practical application of the Data Protection Acts in particular sectors and also by Government when various initiatives are under consideration.

This section gives a comprehensive overview of the Data Protection legislative developments in 2003; describes the activities of my Office during the year; outlines details of significant advice given and some of the principal policy issues which arose.

New legislation

The Data Protection (Amendment) Act, 2003 was passed by the Oireachtas in April 2003 and most of its provisions came into effect on 1 July, 2003 except those relating to enforced subject access and new requirements for registration. It amends the 1988 Act and fully transposes the E.U. Data Protection Directive 95/46EC. The Act strengthens the privacy rights of individuals, clarifies the obligations which fall on data controllers to fairly process personal data and it gives me, as Commissioner, new and additional powers of enforcement. The eight rules of Data Protection, which are outlined on the inside front cover of this Report, are strengthened by this legislation.

What's new in the Act?

New Definitions

- '**Data**' now includes structured manual files as well as computer data. The full effects of the extension of Data Protection Law to manual data will not take effect until October 2007
- '**Personal data**' is any information concerning living individuals
- '**Processing**' is re-defined in a much broader way. 'Processing' means performing just about any operation on information or data - whether automatically or manually - such as: obtaining or keeping data; organising, retrieving, or consulting data; altering or adapting data; using, disclosing or combining the data; and erasing or destroying the data
- '**Sensitive personal data**', which is subject to special safeguards, is now extended to include trade-union membership data.

New rights for individuals

Right to be informed

- An organisation, when obtaining personal data, must inform the individual of (i) its identity, (ii) its purpose for keeping the data, and (iii) any other information required in the interests of fairness - for example, the identity of anyone to whom personal data will be disclosed, and whether or not there is a legal obligation upon individuals to provide the data.
- Organisations who have obtained personal data from a third party - not from the individuals themselves - must, in addition, contact the individuals to inform them of the types of data held, and its source.

Improved Right of Access

- The right of access now extends to both manual and computer data. In addition, a data controller must now also describe the source of the data, and the persons to whom the data will be disclosed.

Right to object

- As an individual, you may request a data controller to stop using your personal data, or not to start using the data (where data are being processed in the exercise of official authority, in the public interest, or for the 'legitimate interests' of an organisation) if you feel that the use of your data involves substantial and unwarranted damage or distress to you.

Freedom from automated decision-making

- Important decisions about you - such as rating your work performance, your creditworthiness, or your reliability - may not be made solely by automatic means (e.g. by computer), unless you consent to this. Generally speaking, there has to be a human input into such decisions.

New responsibilities on data controllers

Publicly available information

- When an organisation is required by law to make a database - such as the electoral register - available to the public, such a database has, up to now, been exempt from data protection rules. The Act provides that an individual must have the right to object to direct marketing where the data has been obtained from publicly available data. (This complements the Electoral Amendment Act 2001 which provides for the establishment, from November 2004, of an edited version of the electoral register in respect of those who have indicated that they do not object to their details being used for non-statutory purposes).

Legitimate processing

- In addition to the traditional rules about "fair obtaining", data controllers will need to comply with additional conditions before data can be processed. In broad terms, such processing will need to be either (i) based upon consent of the individuals; (ii) legally necessary; (iii) necessary to perform a contract to which the data subject is a party; (iv) necessary to protect vital interests of the individual, such as preventing injury, saving life, and preventing serious damage to property; (iv) necessary for a public purpose, such as performance of a statutory function or a public-interest function; or (v) necessary for a private purpose - i.e. for the legitimate interests of a data controller, provided that the fundamental right to privacy is not infringed.

Sensitive data

- In the case of sensitive personal data (such as health details, details about ethnic origin), extra safeguards must also be in place. As a general rule, explicit consent from the individual is necessary.

Journalistic, artistic and literary privilege

- The Act includes special exemptions for processing of personal data for journalistic, artistic or literary purposes, in order to balance the public interest in freedom of expression with data protection rights.

Security*

- Organisations must take all reasonable security measures to protect the personal data under their control, having regard to the nature of the risk involved. Special emphasis is placed in the Act on the requirement that staff be familiar with and comply with the security measures

Transfers of personal data outside of the European Economic Area (EEA)*

- Transfers of personal data outside of the European Economic Area (EEA) will generally be prohibited unless certain safeguards are met. This is because Directive 95/46EC provides a uniform level of protection of personal data within the EEA. In general, such safeguards require the consent of the data subject or a contractual basis requiring the importer to protect the personal data with a level of protection equivalent to that afforded under Irish law.

** These Rules were already in force since April 2002.*

New powers and functions of the Commissioner

Privacy audits

- The Data Protection Commissioner will have the power to carry out investigations as he sees fit, to ensure compliance with the Act and to identify possible breaches. Details of audits and inspections carried out are outlined below.

Prior checking

- The Data Protection Commissioner must consider each application for registration to see whether especially risky or dangerous types of processing (as prescribed in Regulations which have yet to be made) are involved. If so, the Commissioner must establish in advance whether the processing is likely to comply with the Act.

Codes of good practice

- The Data Protection Commissioner has power to prepare and publish 'codes of practice' for guidance in applying data protection law to particular areas. These codes, if approved by the Oireachtas, will have binding legal effect.

Impact of new legislation

Overall, data controllers have reacted positively to the enactment of the amending legislation as they find that the legal requirements have now been clarified. Although the obligations on organisations are now more onerous, it is the objective of my Office to engage with data controllers and help arrive at practical solutions to problems.

I am pleased that in November 2003, the General Practitioner Information Technology Group (GPIT) launched a Guide to the Data Protection Acts for GP's (www.GPIT.ie). This was produced by the Group in association with my Office, the Irish College of General Practitioners the Irish Medical Organisation and gives comprehensive advice on data protection in this sector. It has been favourably received and I am confident that this will be the forerunner to Codes of Practice for GP's and for the Health Services generally. I compliment the Garda Síochána for commencing work to draw up in late 2003 a code for its members and the general public. This is necessary as the Gardaí have sensitive and large databases of personal data which are necessary for it to perform its delicate but necessary tasks and the code will be an assurance to the public as to how personal data is processed.

I am also pleased that the Irish Bankers' Federation have taken the initiative to draft a Code of Practice which their members would follow and this is currently being progressed with the Federation. In the coming year, I hope to progress discussions with interested parties on a Code of Practice covering Data Protection in relation to Employment and Human Resources. I have also discussed with the Insurance Federation the need for a Code of Practice on Data Protection in the Insurance Sector. This is needed as Insurance Companies in both the Life and Non-Life Sectors process significant amounts of personal data, including sensitive data, mainly relating to health and criminal convictions. As in the financial services sector, there is increasing concern about fraud prevention, and while the Data Protection Acts are never a barrier to the sharing of necessary data to prevent fraud, I am asking for greater clarity and transparency in this area.

The privacy in electronic communications regulation 2003

In 1997, the EU introduced Directive 97/66/EC in order to strengthen and clarify data protection and privacy rules in the telecommunications sector. Directive 2002/58/EC replaces and updates the data protection rules for this sector. Directive 2002/58/EC was implemented in Irish law by special Regulations, made by the Minister for Communications, Marine & Natural Resources. The Regulations - known as the European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations, 2003 (S.I. No. 535 of 2003) - came into effect on 6th November 2003. Statutory Instrument 192 of 2002, which transposed Directive 97/66/EC, from May 2002 was revoked.

The new Regulations strengthen the rules on direct marketing and those who contravene these rules are now guilty of an offence that can be prosecuted by my Office. Each unlawful message or call will constitute a separate offence and be subject to a fine of €3,000.

The Regulations set out, in some detail, the data protection standards that apply in the case of public telecommunications networks - including issues of security, privacy and direct marketing. The main features of the Regulations fall into seven categories, as follows:

Retention of detailed telephone records

- Detailed records of people's telephone calls may be kept for as long as necessary to enable bills and telecommunications providers interconnect payments to be settled, but no longer.

Storing and Accessing information on terminal equipment e.g. "Cookies"

- Information cannot be stored on or retrieved from a person's computer or other terminal equipment unless clear information is given to the individual and the individual has the right to refuse the placing or accessing of this information.

Calling line identification or "Caller ID"

- Telephone users have the right to block their phone number, so that it is not displayed to other telephone users. In certain exceptional circumstances (emergencies and garda investigation purposes), people's preferences regarding Caller ID and location data may need to be overridden, so that the number and/or location of the person making the call is available to the person receiving the call.

Location data

- Location data, other than traffic data, can only be processed if made anonymous or with the consent of the individual for the provision of a value added service.

Public telephone directories

- Individuals are to be informed about the purpose of directories. They have the right to be excluded from public phone directories, or to have their address and gender omitted to protect their privacy. If the compiler of a directory has not already done so it must provide information to subscribers currently listed, on the purpose including any embedded search functionality in electronic versions of the directory. If the subscriber does not object to being included in the directory within two months of receiving this information then he is deemed to have consented. The National Directory Database, giving details of those who have opted out of direct marketing, is due to be launched shortly by Eircom under authorisation from ComReg.

Direct marketing

- Unsolicited direct marketing telephone calls, fax messages, e-mail and SMS cannot be sent to individuals unless they have given their prior consent. Individuals can sign up to a central 'opt out' register, to indicate that they do not wish to receive unsolicited telephone calls.
- The Regulations set out the rules for recording subscriber's indications that they do not wish to receive unsolicited telephone calls. This ***national 'opt out' register*** must be consulted by direct marketers, and the wishes of subscribers must be respected. Individuals who wish to be included in

the 'opt-out' register - i.e. individuals who do not wish to receive unsolicited telephone calls - should notify their telecommunications company, which will make the appropriate arrangements. Subscribers with unlisted numbers will automatically be included on the 'opt-out' register.

- The use of ***automatic calling machines***, ***fax***, e-mail or SMS text messaging for direct marketing to individuals, is prohibited, unless subscribers' consent has been obtained in advance.
- Where the subscriber is a customer, e-mail and SMS text messaging can be used for direct marketing purposes if an easy to use, free of charge opportunity is given to object to these marketing messages.
- The use of ***automatic calling machines, fax*** for direct marketing to non-natural persons or businesses, is prohibited, if the subscriber has recorded its objection in the National Directory Database or has informed the sender that it does not consent to such messages.
- The use of ***e-mail or SMS text messaging*** for direct marketing to non-natural persons or businesses is prohibited, if the subscriber has informed the sender that it does not consent to such messages.
- The person making a call shall include in the call their name and on request their address and telephone number. The sender of an e-mail or SMS shall include in the message their name and a valid address at which they can be contacted.

Enforcement and compliance

- The Data Protection Commissioner is the statutory authority for enforcing the data protection aspects of the Regulations, and the Commission for Communications Regulation (ComReg) is responsible for ensuring compliance with some technical and practical elements of implementing the Regulations.

Promoting public awareness

Pending the enactment of the 2003 Amendment Act, my Office's education and awareness initiatives were focussed mainly on data controllers, as we considered that achieving good compliance was how we could best utilise our limited resources. Also, we did not engage in any new education and awareness initiatives for the public as the legislative environment was uncertain. With the passing of the new Act, my Office immediately published three new Guidance Booklets - one setting out what's new in the Amendment Act and the other two aiming to explain the basic points of the legislation for data controllers and data subjects in an easy to follow manner. These booklets are available on our Website and at the end of the year, a re-write of our Website was underway and has recently been completed.

Promoting awareness of Data Protection is one of the key functions of the Office - it is a truism that in order to exercise one's rights, one must first be aware of them. The Public Awareness Survey, details of which were published in my 2002 Annual Report, revealed that while 39% of people had heard of the office, only 9% spontaneously mentioned the Office as a conduit for complaints about invasion of privacy. I regard it as a priority to address this deficiency in awareness, as the Survey also shows that, apart from the legal aspects, the overwhelming majority of people regard privacy as being of paramount importance - only crime prevention was rated more important.

My Office, therefore, has adopted a Public Awareness strategy entailing:

- Collaboration with and speaking engagements at local Citizen Information Centres.
- Interviews on national and local radio and on television.
- Participation in trade shows and other events which will facilitate face to face contact with the public.
- Development of material for inclusion in the Department of Education and Science's curriculum for the Junior Certificate.
- Participation in a Web-site based educational initiative (the Graduate Trail website) for transition year students involving a Data Protection quiz and cash prizes.
- Proactive and reactive engagement with local and national media on Data Protection and related matters.
- Targeted advertising on a sectoral and local basis.

Website information (www.dataprotection.ie)

I regard the Office's website as of primary importance. During 2003, there were 30,000 visitors to the site which displays detailed information on Irish Data Protection as well as providing links to European Union Data Protection Authorities and other Privacy sources. I place considerable store on the value of having it up to date. I am pleased that, recently, the process of updating the guidance material on the site to reflect the new legislation has been completed. In the coming year, I intend to redevelop the site to enable easier and more customer friendly searches so that the public have a ready source of accurate information on their rights. I am also pleased that at the end of the year, the Office's initiative to place an extract of the public register on the web was completed.

Direct contacts - talks and presentations

During the year, 70 Presentations were made by staff of the Office and myself, to organisations in both the public and private sectors, as well as at Conferences, both in Ireland and abroad. In particular, in January 2003, my Deputy and I met with the Joint Oireachtas Committee on Justice Equality and Women's Rights to discuss with them aspects of the Data Protection (Amendment) Bill. At this meeting, I indicated that I would welcome the opportunity of discussing my Annual Report with the Committee on future occasions.

The sectors covered in these presentations during the year included:

- Financial institutions
- Health Boards/Health Authorities
- Government Departments
- Legal firms
- Third level education colleges
- Hotel Industry
- Local Authorities
- IT and Telecommunications

Full details are given at Appendix 6.

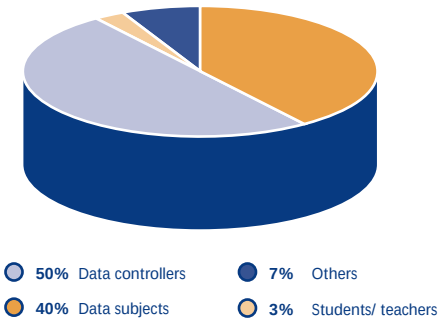
Direct face-to-face contact is a valuable way for my staff and I to engage with data controllers and hear at first hand the practical business problems which may arise in achieving compliance. Equally, these events present us with an opportunity to allay any groundless fears that the legislation may be seen to present. The central message of these talks is always that good data protection is consistent with good record keeping practices and that in the modern environment where customer trust is essential, it can bring competitive advantage.

A major part of the work involves advising data controllers on complex technical and organisational issues around the use and sharing of data, as well as security issues, and regular meetings are held on a daily basis with their representatives. Meetings also take place with Government Departments and industry - in dealings with the latter the issue of developing privacy enhancing technologies which build good data protection into system design and doing privacy impact assessments is at the forefront of my agenda.

Enquiries

Much of the day-to-day work of the Office entails providing information and advice by telephone, (i) as a first step in enabling people to exercise their rights, and (ii) in the case of data controllers, in providing guidance and advice on their obligations. As a public office, customer service is paramount. We have published our Customer Service Plan on the Website as part of our strategy statement, and our internal training places a high degree of emphasis on enabling members of the Office to provide accurate advice and guidelines to telephone callers. Our callers include businesses, public bodies, members of the public as well as people who may be advising others (legal professionals, teachers and citizens advice centres) and the enquiries cover the full range of data protection issues which are within our remit, from calls about individuals' rights to complex enquiries about procedures for transfer of personal data abroad. I would like to commend my staff for their considerable personal efforts during the year to continually update their knowledge, to take account of the new legislation.

Figure 1
Enquiries by caller category



Overall during the year, the office received in excess of 10,000 enquiries, which were fairly evenly distributed between data controllers and data subjects (Figure 1). This is a marked increase on previous years and can be attributed to, (i) an increase in awareness of their rights by the general public and a need for data controllers to be better informed of their responsibilities, and (ii) the capacity of my office to handle more queries, following an increase in staff numbers and the move to our new premises with a much improved telephone system. The queries have tended to be more complex, and reflect an interest in the effect of the new legislation. The increase in enquiries which can be attributed to raised awareness by the general public, is an early indication of a response to the Office's efforts to publicise the new legislation, and it is my objective to build on this in the coming year.

Figure 2
Enquiries by method of contact

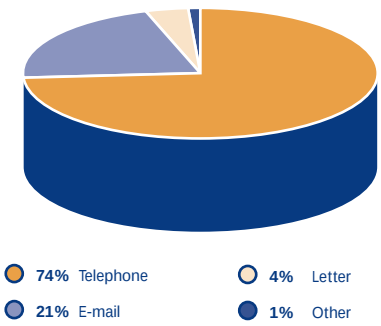
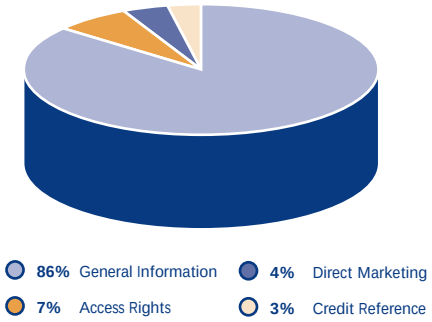


Figure 2 indicates that the new telephone and monitoring systems, installed on the move to our new office, enables staff to, deal with more calls and keep more accurate records. This is now reflected in the statistics, which show that contact by telephone is the main way of interacting with data subjects and data controllers, accounting for 74% of enquiries received.

Figure 3 with regard to the subject matter of enquiries, shows that those seeking general information predominated at 86%. These requests for information covered a wide range of issues and included matters relating to the new legislation, registration, consent, transfers of personal data outside of the EEA, the rules concerning the disclosure of data to third parties, system security requirements and general information on the individuals' rights.

Figure 3
Enquiries by topic



Significant advice given during the year.

The Office provides advice to data subjects and data controllers on the practical application of the Acts. The following are some of the more significant questions dealt with:

Age of consent

The minimum age at which consent can be legitimately obtained was not defined in the Data Protection Act, 1988. A proposal to introduce a minimum age of 18 years in the Data Protection (Amendment) Bill 2002 was not carried forward into the Data Protection (Amendment) Act 2003.

Section 2A(1) of the Acts states that consent cannot be obtained from a person who, by reason of age, is likely to be unable to appreciate the nature and effect of such consent. Judging maturity will vary from case to case.

In the medical area, the GPIT Guide (www.GPIT.ie) suggests that an individual may be assumed to be competent to give consent for medical purposes on reaching the age of 16 years. Where the individual is below that age, consent may still be given, but this requires that the medical practitioner involved must assess whether a child or young person has the maturity to understand and make their own decisions about the handling of their personal health information. In relation to the right of access to health data, where the individual is below 16 years, it was recommended that the general practitioner should use professional judgement on a case by case basis, on whether the entitlement to access should be exercisable by (i) the individual alone, (ii) a parent or guardian alone, or (iii) both jointly. In making a decision, particular regard should be had to the maturity of the young person concerned and his or her best interests.

In the marketing area, where sensitive data is not involved, including on websites, a lower threshold may be permissible. For example, it is a matter for a company to judge if a 14 year old can appreciate the issues surrounding consent and to be able to demonstrate that a person of that age can understand the information supplied and the implications of giving consent. While care should be taken that a person under that age would not be enticed into a deception concerning his/her age, a clear statement that an age limit applies would normally suffice. Where the company becomes aware at a later date that a person has supplied false age-related information, then that data subject's details should be removed from the live site. Sufficient identifiers may be retained purely for the purpose of blocking future entry attempts by that individual.

Where the company accepts that an individual is a minor and are seeking parental consent, e-mail might not be the best medium, unless they can establish that the e-mail address is genuinely a parent/guardian's e-mail address. A postal address is more readily authenticated, though it still does not preclude a letter being addressed to a sibling.

Use of publicly available data for secondary purposes such as marketing

Section 1(4)(b) of the Data Protection Act, 1988 states that the Act does not apply to:

> "personal data consisting of information that the person keeping the data is required by law to make available to the public"

Previously, this provision had been interpreted by this Office as exempting the processing of such data from the provisions of the Act, even in relation to secondary uses of the Electoral Register. This was the basis of Case Study 5 as outlined in the 1997 report.

During the year, advice was given confirming that data obtained from the Electoral Register, from a person who has a statutory responsibility to hold and supply such data, are fairly obtained within the meaning of section 2(1)(a) of the Act. However, if such data are kept by a person who is not required by law to make such data available to the public, then it appears that section 1(4)(b) may no longer apply and it becomes questionable if the data are being fairly processed within the meaning of section 2(1)(a) of the Act.

In regard to personal data obtained for the purposes of direct marketing from a public source, section 2(8) of the Acts now provides that

> "Where a data controller anticipates that personal data, including personal data that is required by law to be made available to the public, kept by him or her will be processed for the purposes of direct marketing, the data controller shall inform the persons to whom the data relates that they may object, by means of a request in writing to the data controller and free of charge, to such processing".

Advice was given to the Irish Direct Marketers Association (IDMA) and others that:

- Where there has been a legitimate business relationship over a period of time with a person, then there is no need to get new consent e.g. banks, insurance companies, loyalty cards and shop special offers etc;
- A legitimate business relationship would be understood to exist where there has been contact within the previous 2 years at most;
- Where a database has been generated from the Electoral Register or other public register, then in respect of existing databases, at the first mailing shot:
  - data subjects should be informed where their name was obtained and that they may object to their name being on the list;
  - a free post envelope should be provided for response;
  - if no reply is received within 21 days, then the name may be used;
  - the notification has to be very precise and in bold type.

Publishing photographs of young people

A youth worker with a National Organisation enquired about their responsibilities in relation to possibly using photos etc. of young people in future publications/promotion. Advice was given that in general, section 2 of the Data Protection Acts requires that data are fairly obtained and fairly processed. To fulfil this fair obtaining provision, a data controller should be able to demonstrate that a person whose data (which includes photographs) are being processed (data subjects) is aware that the data are being processed, as well as being aware of the purpose in processing the data and of any disclosures that are planned. In the case of minors, it was not sufficient to demonstrate that they are aware of these facts and have consented to such processing. It was explained that a minor cannot give consent to the processing of his/her own data and that it would be necessary for a parent or guardian to be informed and consent sought and obtained.

Database of apparently spurious complaints

A National Food Sector Industry Representative Body outlined to my Office that there was a problem with the level of complaints made to member companies by certain individuals who tended to make serial complaints. The Body wished to establish a database which would be accessible by member firms, giving details of people who had made exceptional complaints which the member may have some doubt about. Clearly, the Body would not be able to satisfy the consent requirements of the Acts. I was satisfied that the Industry has a legitimate interest in protecting itself against claims that may not be genuine and was satisfied that the legitimate interests provision of section 2A of the Acts provided a basis for the processing. This provides that personal data may be processed where:

"the processing is necessary for the purpose of the legitimate interests pursued by the data controller or by a third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subjects."

However, I requested that people making complaints to members be made aware of the existence of the database; that their details may be recorded and that they be advised that they have a right of access to this data under section 4 of the Data Protection Acts. I also specified that the data should only be retained on the database for 2 years in the normal course.

Access request to employee personnel records

A major Government Department approached my Office seeking advice in relation to subject access requests received from its own personnel in connection with an ongoing dispute. Because of the nature of the dispute, large amounts of documents had been generated in dealing with the dispute itself. In order to assist the Department in dealing with the access request in a timely manner, my Office took the unusual step of providing a member of staff to view relevant documents and offer appropriate advice. This staff member acted as an agent of the Department and signed an appropriate confidentiality agreement. A number of interesting points arose during this consultation.

- Where a computer system in use does not have a facility to search documents by content, a data controller is not obliged to introduce software to

search documents if that facility is not a feature of the way in which data are normally processed. Such a system would be considered by me to be more like a structured manual file than an automated processing operation.

- The mere mention of a person's name in a document is not always in itself personal data.
- Documents that contained opinions that there was a reasonable expectation were given in confidence need not be released. It might be possible to summarise such documents, or to remove the confidential element. This test would have to be applied on a case-by-case basis, as not all opinions are necessarily confidential; furthermore, a fact given in confidence is not exempt from an access request.
- Data in an employee's own e-mail account is not necessarily his/her personal data just because s/he is the author.
- Certain data can be withheld under sections 5(1)(a) or 5(1)(b) as being prejudicial to an enquiry but each case has to be reviewed separately.

Complaints and investigations

Under the Acts, I may launch an investigation into a possible contravention of the Acts where an individual complains to me that his/her Data Protection rights may have been infringed in any way or where I am otherwise of opinion that there may be a contravention. Where a complaint is received, I, as Commissioner, am required by section 10 of the Data Protection Acts, 1988 and 2003, to investigate it, and, to arrange an amicable resolution. Failing that, I am required to issue a decision in relation to it.

I regard the complaints and investigations function as being of central importance in my Office. Addressing alleged contraventions of the Acts in a proactive manner means that individuals can see that upholding their data protection rights is taken seriously by my Office while organisations where a contravention is established are required to address shortcomings and put new procedures and practices in place. While I have no power to award fines in respect of contraventions, I may issue a formal decision which is subject to a right of appeal by either party to the courts. Individuals who have been the subject of a contravention may make a claim for damages in the courts under section 7 of the Acts.

During the year, it was noteworthy that the nature of complaints being received were increasingly complex, raising, as they did, a range of issues crossing over into other areas of Law, notably Employment and Medical Law, as well as technical and IT issues. Prominent amongst the latter were disclosures of personal data as a result of inadvertent security breaches, underlining the point that no matter what technical and organisational safeguards are in place, the human element must never be overlooked. The increasing complexity of the case-load and the changing Data Protection legal environment caused some slow-down in the processing of complaints. Nevertheless, the additional staffing resources (see under Administration below) that have been allocated to my Office since late 2001 have continued to impact positively on the processing of complaints. During 2003, the number of new complaints processed formally was 258 compared with 189 the previous year (and 78 in 1998). The number of complaints concluded was 199 and at year's end 160 were still on hand. This is illustrated in Figure 4 below.

Figure 4
Complaints received, concluded and not concluded

Figure 5
Breakdown of data controllers by business sector

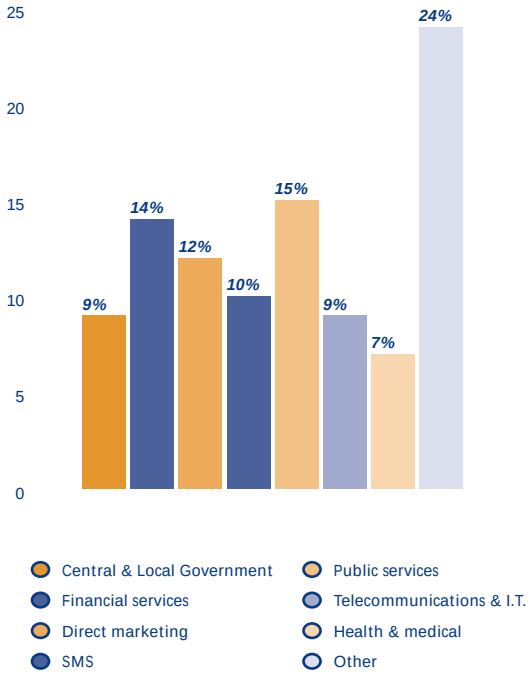


Figure 6
Breakdown of complaints by data protection issue

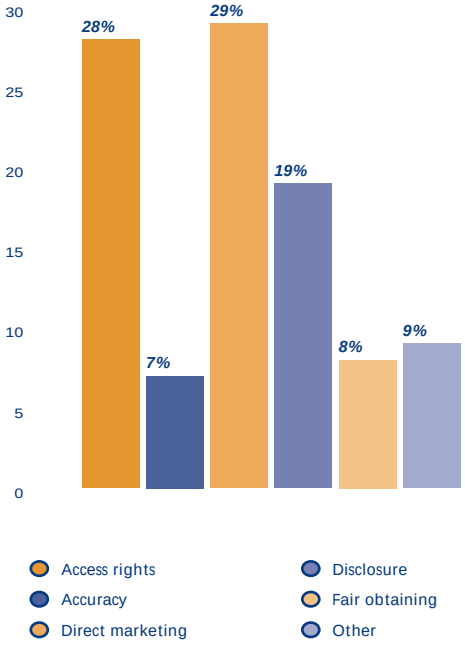


Figure 5 shows a breakdown of the types of organisation against which complaints were made to this Office in 2002. Fourteen per cent of complaints concerned the financial services sector. The Telecommunications / IT sectors accounted for nine per cent of complaints while the direct marketing sector accounted for 22 per cent of complaints. The public services and central and local government also accounted for almost one quarter of complaints.

As regards the grounds for complaint - see figure 6 - the largest single block of cases concerned the exercise of the right of access to data under section 4 of the Act (28%) and complaints about direct marketing (29%). Complaints about the issue of fair obtaining and incompatible disclosures of data to third parties were the next most common issue of complaint (together totaling 27%). Fair obtaining generally involves questions of consent and transparency. One concern often is the "bundling" of consents for uses which are not appropriate to the particular transaction. This means that data subjects are confused and the clarity and transparency that I seek may fall short. It is very important that the consent clause be appropriate to the transaction or service concerned and the envisaged uses of data and that adequate prominence is given to it on the form. Whether or not a disclosure is compatible can generally be answered by the simple test of whether the Data Subject would be surprised by the disclosure. I would, therefore, emphasise what I have said in earlier Annual Reports that unless a data controller is clear and up-front with a data subject, at the time when personal data are obtained, difficulties with data protection law are inevitable.

At the end of the year, 25 complaints received in the 7 weeks following the enactment of the Privacy in Electronic Communications Regulations relating to unsolicited direct marketing via SMS messages were under investigation. It is my intention to take a strict enforcement stance, pursuant to these Regulations, on the whole issue of spamming, for direct marketing purposes, whether by email or SMS.

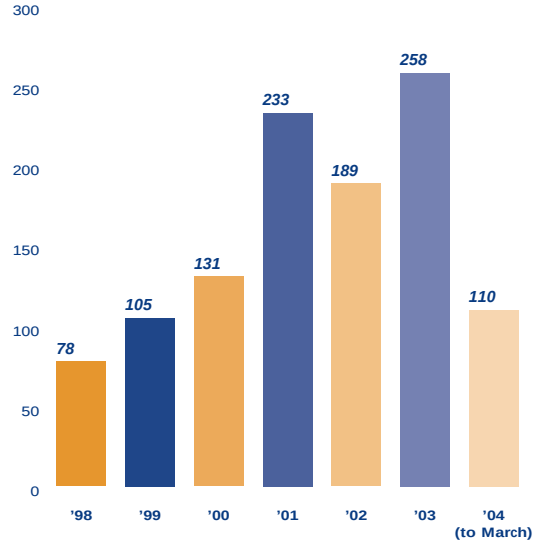
A significant investigation during the year centred on the Department of Communications, Marine and Natural Resources (CM&NR) which commenced publishing details of FOI requests it had received on its website in April 2003, with the exception of requests for personal information. The information initially displayed comprised the name and address of the requester and a synopsis of the information sought. The details of this investigation which involved the issue of an Enforcement Notice against

the Minister and its satisfactory conclusion are outlined in Appendix 2.

Of the complaints concluded, I found that 20% were upheld, 62% were resolved informally while 18% were rejected. Details of the more significant cases are summarised in the Case Studies section in Part 2 of this Report.

Figure 7 indicates the increase in complaints since 1998 is significant and indeed up to mid March 2004 some 110 complaints have already been received.

Figure 7
Complaints received since 1998



Registration

I am pleased to report that there has been a 28% increase in the number of data controllers/processors registered with my Office. The number registered at the end of 2003 was 4,618 as compared to 3,632 and 3,099 at the end of 2001 and 2002 respectively. The extra resources given to this Office has helped in the achievement of these increases.

I consider registration to be of great importance as a means of promoting compliance. Awareness of data protection and the obligations that it imposes on controllers and processors is key. Registration is a very effective measure in raising and maintaining awareness among data controllers. Renewal of registration serves as an annual reminder of data protection responsibilities which is important in an age where staff turnover is high. The discipline of registration requires data controllers to focus on and observe their obligations under data protection law. In particular, they are required to review and describe their processing operations, consider the persons to whom they are likely to disclose data, as well as setting out the security measures in place for keeping data safe and secure. Although the registration system is one of self-assessment, data controllers are bound by law to adhere to the terms of their registered entry.

The sectors in which the greatest increase in registration has been achieved are those that are required to register because they hold sensitive personal data under the Acts. These include the medical profession, pharmacists, the legal profession and schools. I think that registration for those that hold sensitive data is most important as it requires them in particular to outline the security measures they take to ensure that sensitive personal data is not accidentally disclosed or destroyed. In addition there is a misunderstanding in some quarters that data protection responsibilities only apply to those that are required to register. While the registration requirement applies to a subset of data controllers, data protection responsibilities apply to all who control or process personal data. While good progress has been made I aim to further improve compliance with the registration requirement by targeting particular sectors that hold sensitive data.

Before bringing the new registration requirements of the 2003 Amendment Act into effect the Minister for Justice, Equality and Law Reform engaged in a public consultation in early 2004. The period for submissions has only just passed and I made a submission for his consideration.

Prosecutions

At the end of 2003 I initiated proceedings in the District Court against two legal firms in Wicklow and Dublin who failed to register. These two firms were successfully prosecuted in February 2004. The Probation Act was applied and costs were awarded to me in both cases. In addition one firm was asked to pay €500 to a local charity. This action was not

taken lightly. Several letters issued to these firms over a period of months outlining their responsibilities and two on-site inspections were also carried out with no satisfactory outcome.

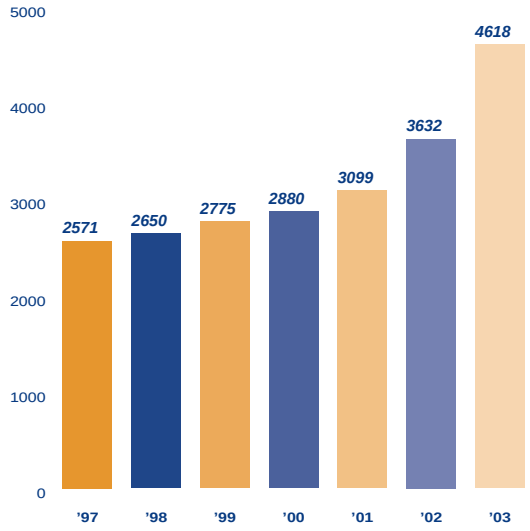
I wish to thank the Law Society, the Department of Education and Science and the Department of Health and Children for their assistance to me in my efforts to have those who process sensitive data on computer registered. They informed those that they represent of the requirement and advised them to register where appropriate but ultimately it is every controller's own responsibility to register.

I intend to prosecute when necessary for similar or other breaches of data protection law in future and it may well be that proceedings in the Circuit Court rather than in the District Court may be taken.

Public register

I am pleased to report that the Register of Data Controllers and Data Processors can now be accessed on-line from my website since December 2003 (See Figure 8).

Figure 8
Register of Data Controllers & Data Processors



Privacy Audits and Inspections

The enactment of the Data Protection (Amendment) Act 2003 gave me the power to conduct investigations where I consider it appropriate to ensure compliance and not only where I have received a complaint or consider that a contravention has or will occur. I prefer my role to be a proactive one rather that a reactive one. I intend to use this authority to carry out "privacy audits" with the main objective of assisting the data controller in complying with its obligations. If shortcomings are discovered then a follow-up inspection will normally be carried out before enforcement notices or the like would issue.

I am pleased to say that my office was able to exercise this authority at an early opportunity. In the latter half of 2003 two privacy audits were carried out. The audits were in a major acute hospital- Beaumont - and in the telecommunications sector- Eircom - and I am happy to say that a high awareness of and compliance with data protection responsibilities was found in both instances.

I intend to conduct a greater number of privacy audits in the coming years. These will be across a wide range of sectors but clusters within a sector will also be a part of the programme. I may engage specialists to carry out particular areas of examination.

Other inspections

During 2003 visits to data controllers were carried out for reasons other than privacy audits. There were nine visits scheduled to legal firms in connection with their possible obligation to register. Eight inspections were carried out as one firm registered in advance of the visit and second visits to three of the firms were also carried out. These inspections were the basis for the successful prosecutions that were taken in the District Court for non-registration which are referred to above in the section dealing with Registration.

On-site visits were made in connection with the investigation of complaints to a pharmacist, a debt collector and a major multinational IT company.

International activities

As I indicated in previous reports Data Protection cannot be confined to Ireland alone. With the ever-increasing globalisation of trade and the advance of the Internet any Commissioner cannot address privacy concerns in isolation. Constant liaison at EU level is beneficial but other regions of the world also provide new insights into how data protection operates. Indeed since the events of September 11 data protection principles worldwide are under review and a sharing of experiences is necessary so as to ensure that these rights are respected even in difficult times. That is why my Office participates in various international fora. Much co-operation is achieved in the normal day-to-day contact between fellow offices with attendances at international conferences kept to the bare minimum.

During 2003 my Office staff and I participated in the following international activities which were of considerable benefit to the Office's operations-

- Article 29 Working Party of the EU member states and the EU Commission.
- EU Supervisory Bodies comprising Europol, Schengen, Customs Information System, Eurodac and Eurojust as well as the related Appeals Committees.
- Schengen evaluation team in Portugal.
- 25th Annual International Conference of Privacy and Data Protection Commissioners in Australia.
- Biometrics Conference organized by the Privacy Commissioner of Victoria, Australia.
- Spring Conference of European Data Protection Commissioners in Spain.
- International Complaints Handling Workshops in Italy and Poland.
- International Working Group on Data Protection in Telecommunications in Germany.
- Annual meeting of the United Kingdom and Irish Data Protection Authorities as well as Guernsey, Jersey and the Isle of Man authorities. (During 2003 an Assistant Information Commissioner -with responsibility for Northern Ireland data protection and freedom of information matters- was appointed by the UK Commissioner and we have had constructive dialogue on matters of mutual interest. We hope to meet regularly to further cross border matters).
- Key note address at the first public forum organized by the newly established Cypriot Data Protection Commissioner.

The Netherlands Commissioner also visited my Office in July 2003.

European union activity

The Office attended all meetings of the Article 29 Working Party, the consultative body comprising the data protection commissioners of the EU member states as well as the EU Commission. The Commissioners of the applicant countries also attended the meetings as observers. The group makes opinions and recommendations on various data protection issues; it tries to have a uniform approach community wide. A lot of time and debate was given to the matter of the USA request for airline passenger data details to be supplied to its authorities and the focus of the Article 29 review was that the measures should be proportionate and with adequate security. I am appreciative of the efforts made by the USA authorities to meet as far as possible our desires but not everything was feasible. However the final agreement with the EU is a far better position than was envisaged in 2002 but it will need to be kept under review.

The Office has continued to provide representation at meetings of the Europol, Schengen, Customs, Eurodac and Eurojust supervisory authorities. In addition my office paid a visit to the Irish liaison office in Eurpol to discuss data protection issues. The office also dealt with an access request to Europol and participated in an evaluation of the Schengen supervisory authority in Portugal. Staff from this office took part in Customs Information System familiarisation session organised by the Revenue Commissioners.

Copies of all decisions made at the EU meetings are available through this Office's website

International conference

The theme of the 2003 International Conference in Australia was "Practical Privacy for People, Government and Business". The aim was that Data Protection Commissioners would be challenged as to their role in the modern world, whether theirs was a constructive role or whether security and business was being impeded by commissioners' actions. Accordingly provocative topics were chosen for debate. I was honoured to be one of the speakers chosen for the session dealing with "a safe and open society - the role of privacy regulators" along with the Police Commissioner from New South Wales and a leading Australian academic. I indicated that such a society is not hindered but enhanced by the actions of a data protection commissioner. The following extracts from my presentation (the detailed presentations at the Conference are available on the Australian Commissioner's website which is linked from this Office's website) summarise the main points I put forward for debate

What does a safe and open society mean?

- Can we communicate freely and in confidence, are reasonable and proportionate responses given, are security concerns paramount, how are difficulties in a modern democracy recognised
- Is the balance right between safety and privacy.

What are the publics concerns?

- Are business, government and law enforcement agencies doing the right thing
- To whom are they accountable and how open is the accountability
- Who gives the necessary independent assurances
- Can it be left to market or indeed self regulation?

Role of Data Protection Commissioner

- Appointed by Government or parliament
- Independent but what does independence really mean
- Makes decisions on complaints or issues restraining orders but could there be adverse reaction to negative ruling against politicians or big business
- Ultimate test of independence - do you compromise for easy life
- Not academic role but practical and businesslike in all respects.

Why create the Office of Data Protection Commissioner?

- Important matter as a human right is involved
- State has dual but contrasting responsibilities - protect citizen/state and facilitate business
- Serious matter if things go wrong for you
- Independent but impartial role that is an enabler for the eSociety
- Point of redress, review, advice, listen and adjudicate
- Accountable to Parliament and ultimately people.

Have Data Protection Commissioners added value to a safe and open society?

- Police matters - Commissioners have a supervisory role but this does not hinder operations
- Inappropriate data on a criminal records system was deleted and safeguards were put in place
- The need that retention of communications traffic data with appropriate safeguards was raised and pursued
- Medical records and marketing concerns were highlighted
- Function creep awareness was targeted
- Stimulated debate in many areas
- Taken a practical approach to serious issues such as the USA passenger data matter
- Took a practical approach rather than a 'theological' approach in highlighting serious issues which were later remedied.

What Data Protection Commissioners cannot do?

- Commissioners are creatures of law and do not make the legislation
- Parliament legislates ultimately and legislation enacted may not be the most privacy friendly
- Balance between privacy and other interests of society is finely drawn and complex while Commissioners observations may not be acceptable to legislators - indeed on occasions Commissioners observations may not be sought
- Government, Industry and Commissioners must be in constructive dialogue with cooperation and respect for each other - not a closed dialogue by either side.

Future role for Commissioners

- Delighted if market forces were the ultimate solution but have we reached that stage
- Data Protection Commissioners have to recognise and respond to responsible and well grounded initiatives whether by industry or governments
- Public credibility needed for eSociety and data protection law enables and empowers
- Commissioners can be the citizens last line of defence to an extent with ultimate access to the Courts
- Partnership role not to be undervalued, a need for regulation still exists while co-regulation can be of benefit to the person
- A safe and open society is not hindered by a Data Protection Commissioner's action and without a Data Protection Commissioner what would the situation
- Ensuring that a human right is respected is the ultimate test for everyone.

Administration

Costs of running the office in 2003

	2003 (€)	2002 (€)	% change
Overall running costs	1,202,733	815,173	48%
Receipts	455,439	350,666	30%

The increase in running costs was mainly due to once - off costs associated with the move to new Office accommodation and higher on-going running costs due to more compliance activity. A fuller account of receipts and expenditure in 2003 is provided in Appendix 7.

Staffing

The full authorised complement for the Office is 21 and the filling of all of these posts is vital if the Office is to be able to adequately discharge the additional workload which the new Act is generating. At the end of the year there were 3 vacancies and while I appreciate the pressure on resources in the public service, the filling of these vacancies is necessary if the Office is to continue to develop and provide an important public service in the pro-active way which we are seeking. I wish to acknowledge the continuing positive response of the Department of Justice, Equality and Law Reform and their understanding of our needs in this regard.

Performance management development

In October 2003, the Office submitted the necessary Progress Report to the Justice and Equality Sector Performance Verification Group which assessed the Office's progress in relation to its commitments which had been agreed under its Modernisation Action Plan. The significant elements of this Plan are:

- **Customer Service:** Giving prompt and accurate advice to personal callers, either in person, by phone or email, is crucial not only to service delivery but to the public image and status of Data Protection. We are following several initiatives to build on our strong customer service ethos, particularly in the areas of delivering services over the internet and targeting our message in a clear and simple manner across the country at local level.
- **Equality:** We seek to disseminate and build awareness of Data Protection across all sectors of society and in particular to promote and encourage access to our service for people who may otherwise feel excluded from the world of computers and e-business. Within the Office, staff have availed of parental leave and job sharing and the Office culture is fully supportive of these family friendly initiatives.
- **Staff Training and Performance Management:** In pushing forward with Modernisation, I am firmly of the view that the most important resource is staff. My policy is to provide an environment where every staff member is both given the opportunity and encouraged to develop their full potential and also where they feel included as part of a team. Staff morale and customer service have been boosted by our move to new accommodation last May. We are currently engaged in internal training to develop staff expertise in the new legislation and we see the development of performance management, with its emphasis on clarification of roles and training, and its link to the Business Plan, as making a key contribution to expertise.
- **A Partnership Committee:** was established, comprising of 5 staff - one person nominated by staff from each Grade in the Office - to support, and involve staff in, the development of the Office. The Committee has played a positive role with our Action Plan. They have a general brief to look at work organisational issues and training. While staff are encouraged to make their views known at regular staff meetings, which I chair, it has been found that this smaller Group has worked well, in increasing communications at an informal level between staff. Some new initiatives are being developed as a result of discussions at this Committee, in particular shaping our approach to the education and awareness strategy. Other staff are also encouraged to contribute, updates are circulated after every meeting and staff are invited to attend as observers, for their own development, and for the purposes of transparency.
- **Efficient use of resources:** The additional staff assigned to the Office over the last 2 years, has enabled more thorough compliance activity, particularly in regard to registration requirements as some 4,600 controllers have now registered (3,600 in 2002 and 3,000 in 2001) and in clearing complaints. More and more use is also being made of IT to enhance use of resources.

I was pleased that the Performance Verification Group informed me in December 2003 that the progress achieved in relation to the Office's commitments warranted the payment of the pay increases due from 1 January 2004 to all grades of staff in the Office. I very much appreciate the commitment and support of the staff during 2003.

Support services

The technological environment within the Office was reviewed during the year. Operating Systems, software and some of the hardware was upgraded which should serve the office for the next few years. I wish to record my appreciation for the ongoing services provided by the Department's IT personnel. I am also happy to record my appreciation of the Department's Finance Division, based in Killarney, which has continued to provide my Office with a vital service in the area of receipts and payments.

part two

Case Studies

Case Study 1

Drogheda Hospital - investigation into a consultant's practice - patients felt consent was necessary - balance to be struck with concerns for public health issues overall

I received many complaints from former patients of a Drogheda hospital in relation to the manner in which an investigation was carried out by a health board into the conduct of a consultant's practice. They complained that in the course of its investigation, the health board had sent copies of patients' records and charts to a UK based healthcare risk management group and to an Irish review group without the consent of the individuals involved in 1998 and subsequently.

When I began to investigate the matter, I established that the data that had been disclosed by the Health Board prior to1 July, 2003 was manual data, consisting of patient files, theatre files, etc. While the Data Protection Act, 1988 only applied to personal data on computer the Data Protection (Amendment) Act, 2003 applies to manual data from 1 July, 2003. Whilst manual data, therefore, was involved, and was not subject to the remit of my Office as the manual data in question was referred in 1998, nevertheless, given the major issue involved, the matter was given full consideration as if the principles of both Acts applied.

The background to these complaints was that in October, 1998 the Health Board was made aware of serious concerns in relation to the management of patients under the care of a Consultant Obstetrician/ Gynaecologist, as a result of which a preliminary assessment was carried out in relation to the perceived concerns regarding his clinical practice. The records of 42 patients were involved and to ensure patient privacy and confidentiality, patients were numbered consecutively and this numbering was used in the management of all subsequent classifications in the review process.

Initially the records of 3 patients were sent to the UK based company for risk assessment review. Consultation was then undertaken by the Health Board with the Chairman of the Institute of Obstetrician and Gynaecologists in Ireland, who indicated that the Institute would assist the Board in order to conduct a review. The Board stated that it was their intention to deal with the alleged serious concerns regarding the Consultant and his practice in a confidential and sensitive manner, having regard to the Board's statutory duty of care and service management to patients availing of services within its area. The Review was carried out by the Institute at the request of the Health Board, and consisted of three independent Obstetrician Gynaecologists. The Terms of Reference included a request to assess and consider the nature and merit of the concerns of the Health Board.

The Health Board maintained that it had a duty of care to patients within the Health Board area and when it was appraised of serious concerns relating to patient care, immediate legal and medical advice was sought and that it was in this regard that charts were provided in a confidential manner to the Review Group following consultation with the Institute of Obstetricians and Gynaecologists. It also stated that at this stage the well-being of patients and the wider population was the primary concern. The Health Board set up help lines and counselling services, following the significant media coverage of the concerns in December, 1998 regarding the consultant's practice. Following receipt of the Review Group's Report in April 1999, the help-line was re-activated and direct contact was made with the General Practitioners of patients involved by way of letter and telephone, who were asked to advise patients directly about the report and the options available to them.

> Having regard to the serious and far-reaching public health issues and circumstances involved, I considered that the Board were justified in making the disclosures under section 8(b) and section 8(d) of the Acts

The general principle of the Data Protection Acts is that personal data should only be processed and disclosed to other parties with the patient's consent unless one of the provisions of section 8, which lift the restrictions on disclosure in limited and defined circumstances, apply.

Section 8(b) provides that -

> *"8. - Any restrictions in this Act on the processing of personal data do not apply if the processing is -*
>
> *(b) required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders or assessing or collecting any tax, duty or other moneys owed or payable to the State, a local authority or a health board, in any case in which the application of those restrictions would be likely to prejudice any of the matters aforesaid..."*

while section 8(d) provides that -

> *"8 - Any restrictions in this Act on the processing of personal data do not apply if the processing is-*
>
> *(d) required urgently to prevent injury or other damage to the health of a person or serious loss of or damage to property."*

Section 8 therefore recognises that privacy rights are in no sense absolute and must constantly be balanced against other competing interests including society's right to be made aware of particular information.

The matter which had to be considered by me, therefore, in terms of the Data Protection Acts, was whether the Board could rely on any of the provisions of section 8 as a basis for the referral of case files to the UK company and subsequently to the Enquiry by the Institute of Obstetricians and Gynaecologists, without the consent of the patients involved.

In routine referrals anonymised information should only be disclosed; charts etc might not need to be forwarded and indeed prior patient consent should be sought. However, **in a case such as this when a serious matter, with implications for the health and welfare of past patients and indeed possible dangers for current and future patients, was brought to its attention, I deemed that the Board had a duty to fully establish all of the facts using whatever expert resources were necessary and indeed in a speedy and urgent manner**. I considered that the Board were justified in disclosing the files in order to protect the health of those who had had the procedures carried out by the consultant and also so that necessary steps could be identified to avoid inappropriate procedures in the future. Having regard to the serious and far-reaching public health issues and circumstances involved, I considered that the Board were justified in making the disclosures under section 8(b) and section 8(d) of the Acts.

Furthermore, I considered that the disclosure by the Board was a compatible disclosure within the meaning of section 2 of the Acts. Section 2 (1) (c) (ii) provides that "data shall not be further processed in a manner incompatible with that purpose or those purposes" (for which it is held). I considered that **the disclosure of patient data for the limited purpose of practice review in the wider interest of public health and, subject to confidentiality and privacy safeguards, was consistent with the purpose for which personal data was held by a healthcare provider**. However, while names of patients were also included in the charts supplied to the reviewing bodies it would have been prudent, if it were feasible, given the urgency and importance of the investigation, to delete all references to patients so that only anonymised information was released.

I deeply appreciate and I am glad that the matter was brought to my attention by concerned and reasonable patients as it raised serious matters in the healthcare area regarding data protection.

Case Study 2

PMI Ltd mailing list rented in good faith by a bank resulted in minors being marketed for credit cards without proper consent

In early January 2003 I received a complaint from an individual to the effect that his ten year old daughter had received unsolicited mail from a bank offering her a credit card. The letter was addressed to the child using "Blackrock, Co. Dublin" as the postal address. However the use of "Blackrock, Co. Dublin" indicated to the complainant that the address was not provided by any member of the family as they always used "Stillorgan, Co. Dublin" in their correspondence. The complainant contacted the bank in the matter requesting an explanation and also that his daughter's name and that of his immediate family be removed from its mailing list. He was informed that the mailing list used by the bank had been rented from Precision Marketing Information Ltd.(PMI) who had got the details from a reputable third party.

The bank phoned my Office when this matter arose and stated that a mailing list, obtained from PMI, apparently had included data relating to a number of minors. The bank had issued credit card marketing material using this list and, in the process, had inadvertently marketed a minor. PMI also informed my Office that the maximum number of minors' records involved in this instance was 202 and that those records were in the process of being deleted.

As there appeared to be a contravention of the Data Protection Acts, I then investigated the matter under section 10 of the Acts.

I established that the data purchased by PMI from a UK Company was obtained by that company from a post-holiday survey form which include age categories. The information was held and processed by the UK Company with whom PMI had an agreement to purchase data relevant to residents of the Republic of Ireland. However in this instance, the data relating to a minor arose as a result of a coding error when loading the new data onto PMI's systems. The error was rectified and additional stringent checks were put in place to ensure that an error of this type never occurred again.

the standards of fairness in the obtaining and use of minor's data, required by the Data Protection Acts, are much more onerous than when dealing with adults. I consider that use of a minor's personal data cannot be legitimate unless accompanied by the clear consent of the child's parent or guardian

Under Data Protection legislation fair obtaining of personal data is an active duty. It is up to the data controller, not the data subject, to make sure that it takes place. For a data controller to satisfy the requirements of fair obtaining and purpose specification it must ensure that at the time of providing personal information, individuals are made fully aware of:

- the identity of the persons who are collecting it (though this may often be implied),
- to what use it will be put,
- the persons or category of persons to whom it will be disclosed.

I consider that when dealing with personal data relating to minors, the standards of fairness in the obtaining and use of data, required by the Data Protection Acts, are much more onerous than when dealing with adults. I consider that use of a minor's personal data cannot be legitimate unless accompanied by the clear consent of the child's parent or guardian.

In this case, the minor's details were not fairly obtained in contravention of Section 2(1)(a) **as a ten year old cannot give valid consent even if the opt-out box has not been ticked**. The coding error resulting in the incorrect entry of the child's details onto PMI's systems was in contravention of Section 2(1)(b) as PMI, albeit inadvertently, supplied data relating to minors to the bank and this led directly to the mailing received by the child in this case.

I considered the point made by PMI that they rather than the bank were the data controller in this case. While PMI were the original Data Controller of the

mailing list however, when it came into the hands of the bank, through renting it, the bank then became the Data Controller of the list. While the bank actually mailed the minor, I accepted that it rented the mailing list, which inadvertently contained the minor's details, in good faith from PMI. I noted that PMI, with whom the bank had a contract, provided it with data which included data relating to 202 minors under18 and as a result the bank marketed the minor in this particular case. **I therefore found that the bank and PMI as data controllers were both in contravention of section 2 with regard to fair obtaining, processing and use of the minor's data in this instance**.

I was satisfied that PMI were aware of their responsibilities under the Data Protection Acts, 1988 and 2003 with regard to the use of data for direct marketing purposes, particularly in regard to minors. I accepted their assurance that the coding error which gave rise to the complaint was rectified and that additional stringent checks were put in place to ensure that an error of this type would not occur again. I acknowledged the swift action taken by both PMI and the bank in response to the complaint and to their co-operation with my Office in the course of the investigation.

While I also accept that the bank was the innocent party in this instance nevertheless marketing companies must take reasonable but effective measures to ensure that minors are not the targets of marketing campaigns without proper consent. See page 17 for advice given during the year relating to Data Protection and Minors.

Case Study 3

Visa application details accidentally put on website of Department of Justice, Equality and Law Reform

A journalist contacted my office with urgent concerns regarding the publication on a website of personal details of visa applicants. I investigated the matter and found that the personal data of visa applicants had been displayed by the Immigration & Citizenship Division of the Department of Justice, Equality & Law Reform on the Department's website on 6 February, 2003. It appeared that through an unfortunate and accidental breach in operating procedures, visa decisions for 506 applicants were posted live on the website with the inadvertent inclusion of the applicants' name and nationality. The data had been accidentally on the website for about two hours but as soon as the error was noticed the details were deleted.

This situation arose as a result of a decision to revise and improve the visa process. It was considered of benefit to place non-personal visa decision information on the website as it would be of merit to staff and visa applicants to have 24 hour easily accessible information available on the website which would reduce the need for applicants to contact the section. It had been agreed that no personal details would be shown; the only information to be posted would be the visa application number, the decision and, where an application was refused, the reason for the refusal.

Due to an operational oversight, the personal details were included contrary to the Department's intention. Accordingly, this was a contravention of Section 2(1) (c) of the Acts, being an incompatible disclosure of personal data. Appropriate security measures were inadequate and constituted a contravention of section 2(1) (d) of the Acts.

I note and appreciate that this accidental and unfortunate action was a once off which was swiftly resolved by the immediate action taken by Immigration & Citizenship Division. Nevertheless inappropriate disclosure took place for a short period. I was assured that new procedures were put in place for any future postings on the website which would avoid a recurrence of this incident. I commend the Division for its response.

> advise all data controllers to take special care when it is proposed to place personal data on a website. Even where there is legislation providing that information must be made available to the public, this need not always mean that it is appropriate to place such information on a website

On a more general level I would strongly advise all data controllers to take special care when it is proposed to place personal data on a website. Even where there is legislation providing that information must be made available to the public, this need not always mean that it is appropriate to place such information on a website. Consideration must be given to the balance required between the right of the public to certain information and the right of the individual to privacy. Sometimes it may be appropriate to inform the public by means of information on a website, without disclosing personal details. **These rights have to be balanced, and I would encourage data controllers to have procedures in place to ensure that adequate consideration is given to these matters. Furthermore security procedures must be adequate and staff must be aware of and implement them so as to avoid the occurrence of a situation as described in this case study**.

Case Study 4

Access to medical records on a change of general practitioner

A person contacted me regarding her difficulty in obtaining her actual medical file which she had formally requested from the local Health Centre under section 4 of the Data Protection Acts. She explained that she was a private patient of a doctor at the Centre which catered for General Medical Service's patients - the doctor treated patients on a private basis also. Her doctor had left the practice and had passed her records to his replacement in the Centre. She had received advice from her local Health Board that, under normal protocols, files associated with a general practitioner would transfer to the successor on the General Medical Service's panel. However, files relating to private consultations between an individual and their general practitioner were a different matter. This is an important and correct distinction in Data Protection Law because the patient was a private patient. **The doctor is therefore the data controller in respect of private patients and not the Health Centre or the Health Board**.

In the course of our investigations, my Office established that the replacement GP had offered the complainant a copy of her medical notes but not the actual file, which is consistent with his obligations under the Acts. He had taken legal advice regarding the transfer of her notes to him and was satisfied that he, as a principal of the Health Centre, was entitled to custody of the complainant's file.

My Office informed the complainant that she had a right, under section 4 of the Acts, to access her data, but did not have a right to obtain her actual file. I also advised that if she wished to transfer as a patient to another practitioner outside the Health Centre, she could request that a copy of her medical records be sent to her new GP. However, the GP at the Health Centre is entitled to retain custody of her file for medico-legal and other professional requirements.

General Practitioners are at the coal face of the medical service and patients are happy to put confidence and trust in them regarding their personal data. A health service can be delivered in an efficient and effective manner while at the same time respecting peoples' privacy. The general nature of data protection law, to the extent that it leaves scope for ambiguity, entails a certain lack of legal certainty and clarity. For this reason, I liaised with the Irish College of General Practitioners and the National General Practice Information Technology Group which led to the timely publication in November 2003 of "An Information Guide to the Data Protection Acts for General Practitioners". The Guide addresses the issues surrounding custody of patients' data raised in this case and advises that **General Practitioners should take prompt reasonable steps to notify patients of cessation of practice and allow them the opportunity to transfer their health information to another provider**. It also says that:

> "where a patient decides to transfer to another doctor, the existing doctor should, in accordance with data protection law and ethical guidelines, facilitate that decision by making available to the patient's new doctor a copy of the patient's health information. The existing doctor should, however, maintain the patient information record accumulated at that time for an adequate period consistent with meeting legal and other professional responsibilities. During that period, the provisions of the Data Protection Acts continue to apply to that information."

In this case, I was pleased that the newly appointed doctor was following the guidance on the transfer of records. The case also highlights the important distinction between a data controller in respect of public patients (which is the Health Board or hospital or Health Centre as the case may be) and private patients (which is the relevant health professional).

highlights the important distinction between a data controller in respect of public patients (which is the Health Board or hospital or Health Centre as the case may be) and private patients (which is the relevant health professional)

Case Study 5

Realm Communications - Unsolicited SMS texting and direct marketing

I received a number of complaints from people who had received unsolicited mobile phone text messages from Realm Communications offering a free stay in one of 30 Irish Hotels. The text messages were sent during the summer of 2003 when S.I.192/2002 was the operative legislation in this area. Regulation 9(1) of that statutory instrument states:

> "A person shall not use, or cause to be used, any publicly available telecommunications services to make an unsolicited call for the purpose of direct marketing by means of an automated calling machine or a facsimile machine to the line of a subscriber, who is an individual, unless the person has been notified by the subscriber that for the time being he or she consents to the receipt of such a call on his or her line".

The complainants had not given their consent and the sender did not dispute this. From my investigations it was established to my satisfaction that the **means of sending these messages was an automatic process**. The content of the message, offering the free stay in a hotel, I considered to be direct marketing.

S.I.192/2002 implemented the provisions of Directive 97/66/EC. Article 3(1) of that Directive which is referenced in Regulation 3 of the S.I. states that "This Directive shall apply to the processing of personal data in connection with the provision of publicly available telecommunications services…".

Realm Communications claimed that it was not processing personal data and for that reason the Regulations did not apply. It explained that it had a database of anonymous mobile numbers. Those who responded to the message were required to telephone a premium rate number. When they did so they were given a randomly generated claim number and their mobile number was deleted from its database. It was only at a later stage that personal details were recorded by the hotel on quoting the claim number. It maintained that personal details were never provided to or recorded by the sender of these messages or associated with the mobile numbers on its database.

> The fact that personal details were never provided to or recorded by the sender of these messages… was not central to the overall issue of unsolicited text marketing

I could not accept this argument as I considered that it was not central to the overall issue of unsolicited direct marketing calls being made which are governed by regulation 9 of S.I.192/2002. To restrict the interpretation of the regulations in such a way would, in my view, require a reading of Regulation 9 contrary to its literal meaning. It is a well established legal principle in Irish Law that where the literal meaning of a provision is clear, that is the meaning which should be attributed to it.

The sender probably earned a substantial amount of money from this promotion through premium-rate-call charges and framed the operation of the promotion in an attempt to technically circumvent the regulations. I decided that his actions were covered by the regulations and that he contravened those regulations. I wish to acknowledge the assistance of Regtel - who supervises the premium rate regime - in the conduct of this investigation.

Since the decision on this complaint the Regulations have been superseded by S.I.535 of 2003 which implement the provisions of Directive 2002/58. These Regulations strengthen the law on unsolicited marketing by SMS text, e-mail, fax or telephone. **For the purposes of these new Regulations a person's phone number or e-mail address alone is considered to be personal data. These Regulations also make it an offence to send unsolicited marketing messages without prior consent and I have the power to prosecute these offences**. There is a maximum fine of €3,000 for each message sent.

Case Study 6

Inappropriate disclosure by a headhunting firm of a person's CV to his current employer

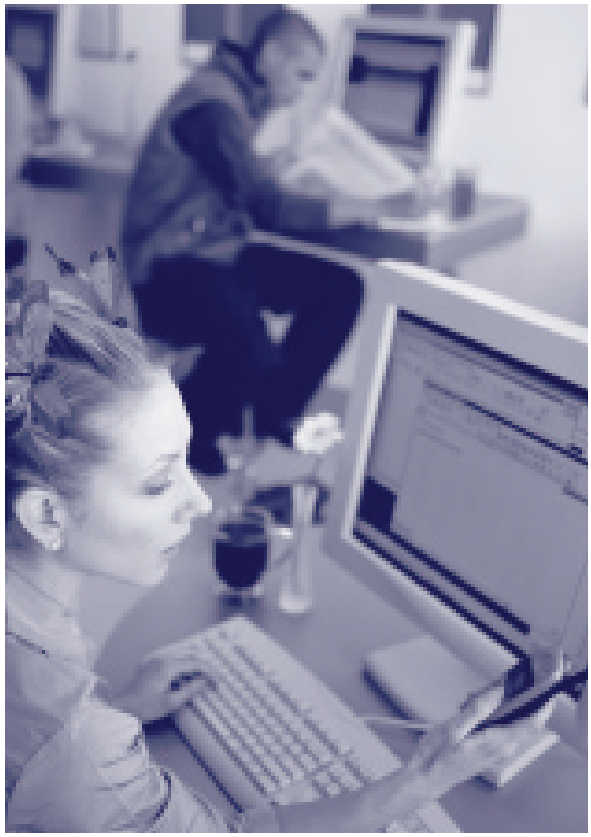
I received a complaint from a Technician Engineer and Project Management Practitioner in the specialist areas of Civil, Structural and Construction Engineering. For some months previously, he had been seeking a career change. He submitted his CV and covering letter to a particular Recruitment Agency, with a view to them distributing these documents to companies of interest to him, with his prior consent. However, he stated that the Agency submitted his CV electronically to his current employers, without his consent, resulting in embarrassment for him and damage to his career and good name.

The company responded that the substance of the complaint was correct. They stated that they had a well established track record in the recruitment business over many years and had a database of many thousands of professionals. They had a high volume of transactions and their processes are that CVs are only submitted to clients with the express permission of the individuals. They also stated that all their recruitment consultants receive training in relation to Data Protection and they also employ a controller whose job is specifically to manage the database software which is used to store and manage CVs.

The company explained that what happened in this case was that a junior consultant, who was filling in for a senior consultant on leave, did not follow the company regulations regarding the distribution of CVs. This incident was the first such complaint that they had had in their entire business history. They had apologised to the complainant and had at his request removed his data from their records. The company said that they believed that the very clear notations on both the working copy of the CV and the database record should have been sufficient to prevent the sending of the CV to the complainant's employer but that in this instance, there was an instance of human error. Since the incident, the senior recruitment consultant has implemented a system of rigorous verification before CVs leave the 'outbox' of any of their employees' email accounts.

I found that the individual's personal data was disclosed by the company to a third party without his consent and that the company also breached the security requirements of the Acts as adequate safeguards were not in place. While it was an isolated incident nevertheless it was a source of considerable distress to the individual. In any human resource matter but especially in sensitive areas the level of security must be paramount and all staff must be aware of their responsibilities. Can one imagine what the consequences would be if say medical data were disclosed in a similar manner?

In any human resource matter but especially in sensitive areas the level of security must be paramount and all staff must be aware of their responsibilities. Can one imagine what the consequences would be if say medical data were disclosed in a similar manner?



Case Study 7

Aer Lingus - Payroll data was not disclosed inappropriately when not paying Impact trade union members' wage increases

Three employees of Aer Lingus complained that information held on the Aer Lingus payroll database regarding their authorisation to allow deductions at source in respect of their union subscriptions was used by Aer Lingus to identify and single them out as IMPACT members and deny them pay increases and refuse them staff travel privileges. They felt that Section 2 of the Data Protection Acts which provides that personal data obtained for one or more specified, explicit and legitimate purposes was breached as their payroll data was further processed in a manner incompatible with the purpose for which it was given i.e. solely to deduct union subscriptions.

On enquiry **my Office established that Aer Lingus did not refer to the payroll database in this instance**. In May 2003 it reached agreement with SIPTU on work practice changes in return for the 4% and 3% pay increases provided for under national pay agreements. Agreement was not reached with IMPACT on work practice changes, so Aer Lingus decided that these pay increases would only be applied to SIPTU members. SIPTU supplied a list of their members to facilitate payment of these increases. Accordingly, I considered that the complaints were without foundation and that no contravention of the Data Protection Acts had occurred in this instance.

This contrasts with the details outlined in case study 2 of my 2000 Report where the Department of Education and Science used trade union membership subscription data to withhold pay in an industrial dispute and indicates that Aer Lingus was fully aware of its Data Protection responsibilities.

I considered that the complaints were without foundation and that no contravention of the Data Protection Acts had occurred in this instance

Case Study 8

Catholic Church baptismal records deletion request not upheld

I received a complaint during 2003 from an individual living in the Netherlands who stated that he had contacted the parish priest in a Catholic church in Ireland where as a baby he believed he had been baptised in 1978. He had requested to have his name removed from church records and that his request had been refused on the grounds that it was not possible to be removed from the church register. He stated that he never joined the Catholic church; his parents had enrolled him without his consent; he now wished to distance himself from it and there was no longer any need for the church to keep information about him.

On investigation of the complaint, the Parish Priest advised my office that a thorough search of the Baptismal Registers for the year in question and for the years before and after that, had failed to reveal a record of the complainant's baptism. The Priest came to the conclusion that it appeared that the complainant may not have been baptised in that parish, and advised that should he provide documentary evidence, for example, a copy of a Baptismal Certificate, then the matter would be investigated further. He also indicated that he would be willing to note the record that the person no longer wished to be associated with the Catholic church or to be classed as a Catholic.

With regard to his request to have his data deleted from the Register, should the relevant record be identified by him, it is my understanding that the data could not be deleted from the Register as it is essential for the administration of Church affairs to maintain a register of all the people who have been baptised. Indeed it is of course a factual record of an event that happened. However the proposed noting of the register would more than comply with Section 6 of the Data Protection Acts, 1988 and 2003. I considered the approach taken by the Parish Priest to be both appropriate and considerate.

I communicated this information to the complainant but the matter has not been pursued further.

.

it is my understanding that the data could not be deleted from the Register as it is essential for the administration of Church affairs to maintain a register of all the people who have been baptised. Indeed it is of course a factual record of an event that happened.

Case Study 9

Referral of medical consultant's clinical notes for review without his or the patients' consent

A medical consultant complained that a health board had sent the clinical notes of five of his patients to a risk management group in England in March, 2000. His consent was not obtained for the release of his patients' personal information while it also appeared that patient consent was not obtained.

On inquiry by my Office the health board stated that following the appointment of a temporary consultant in his place, concerns were brought to the attention of the General Manager of the Hospital, who in the interests of care to patients requested an independent assessment of the concerns raised. The Health Board requested the assistance of an English healthcare risk management group in relation to a review of the patients' treatment specifically in the area of internal medicine and cardiology and to advise if the concerns were justified. The board also stated that the patients' consent was not requested as it was an assessment considered necessary in relation to the concerns raised, and that legal and medical advice was obtained in relation to the matter. The patient charts were treated in a confidential and a sensitive way, with circulation restricted. The outcome of the assessment was that the concerns raised were not significant in relation to the treatment and care of the patients.

As outlined in case study 1 in a case such as this when concerns, with implications for the health and welfare of patients, were brought to its attention, **the Board had a duty to fully establish all of the facts using whatever expert resources were necessary and indeed in a speedy and urgent manner**. Having regard to the public health issues involved, I considered that the Board was justified in making the disclosures, in order to have the risk assessment carried out and did not breach the Data Protection Acts.

In this case and indeed for patients in acute public hospitals it has to be recognised that the health board or the hospital is the data controller and not the consultant. However where a consultant has private patients then he/she becomes the controller if he/she is treating them in a private hospital or in his/her private rooms.

I considered that the Board was justified in making the disclosures, in order to have the risk assessment carried out and did not breach the Data Protection Acts

Case Study 10

Department of Social and Family Affairs market research survey on customer satisfaction by an agency did not breach Data Protection provisions

> This case gives a clear insight that data protection law does not prevent a properly managed customer satisfaction survey being carried out by an agent acting for a data controller

An individual complained that the Department of Social and Family Affairs (DSFA), had disclosed her name and address to the Market Research Bureau of Ireland (MRBI) for the purposes of conducting research and that subsequently, a representative of the MRBI visited her home to conduct an interview. She felt that the Department had breached the Data Protection Act 1988 and had made her data available without her consent to a private firm.

On investigation of the complaint, the DSFA confirmed that it had commissioned MRBI to carry out a national survey, on their behalf, to see in what way their service could be improved upon. MRBI, acting as an agent for the DSFA, were given a list of customers' names and addresses that were selected at random from DSFA databases for the purpose of this survey only. These people received a letter from the Department informing them about the survey, and indicating that data provided in interviews would be held in the strictest confidence by MRBI and that the names of those participating would not be disclosed to the Department. A box at the bottom of the letter contained the following statement -

> "In line with the Data Protection Act I would like to assure you that the MRBI is carrying out this survey as an agent of the Department. MRBI has been required to fulfil the following conditions:
>
> - To hold the Department's list only for as long as is required to complete the survey and thereafter to delete the list from all their records.
> - To ensure that their interviewers make no attempt to recruit any of the Department's customers for any other survey."

I noted that the letter which issued in advance of the commencement of the survey gave people an opportunity to contact the Department if they had any concerns. I obtained a copy of the contract between the Department and MRBI which confirmed that MRBI would adhere to the terms of the Data Protection Act.

The Department is not prohibited by the Act from using personal data for the purposes of its own research, such as a survey, even where the data subject was not informed in advance, provided that no damage or distress is likely to be caused to the individual. Section 2(5) of the Act provides for this.

It is a matter for the Department to decide whether it wished to carry out the research or to contract another party to carry it out. Thus, **where a data controller wishes to carry out a task which is within its competence and authority to do but assigns that task to another person and makes available, to the other person, personal data for the purpose of that task and that task only, this is not considered to be a "disclosure" within the meaning of the Data Protection Act. In no circumstances may the data be retained by the agent once the task is completed**.

I noted that the Department adhered to the Act by having an appropriate contract with MRBI. Accordingly, **the transfer by DSFA of data to MRBI for the purpose set out in the contract with MRBI did not constitute disclosure of data within the meaning of the Data Protection Act, and consequently was not a contravention of the legislation**.

In correspondence with my Office, the complainant referred to the Law of Agency and disputed my interpretation that a disclosure by a data controller to an agent does not constitute "disclosure" within the meaning of the Data Protection Act. I did not accept that proposition. Indeed Professor Robert Clark in "Data Protection Law in Ireland", published by the Round Hall Press (1990), stated that:

> "The definition of disclosure excludes a disclosure made, directly or indirectly by a data controller or data processor to an employee or agent of his for the purpose of allowing the employee or agent to carry out his duties'".

In response to my preliminary determination the complainant stated that:

> "I have studied with interest the contents of your decision regarding the apparent acceptable degree of protection that was afforded this DSFA client under Data Privacy Legislation, and most alarmingly, the implied differential civil rights. Not only does all reputable research conform to standardized 'ethical' practices, but in line with such, the process itself in no way over-rides the fundamental rights and freedoms afforded to citizens under Bunreacht na hEireann nor the EU Convention. In light of the nature of your draft decision, I would consider it a time-wasting exercise to make any further observations on this matter".

I was disappointed by this attitude as I only come to my final determination when I have considered all angles. Indeed I request all complainants and data controllers to offer as much argumentation and facts as they consider appropriate before I make a final decision on complaints - hence my practice of issuing a draft decision to both parties for further observations before I make a final decision. My final decisions can be appealed by either party to the Circuit Court. Though the complainant did not exercise her right to appeal or offer further comment on the draft decision nevertheless her arguments were considered in detail.

This case gives a clear insight that data protection law does not prevent a properly managed customer satisfaction survey being carried out by an agent acting for a data controller.

Appendicies

Appendix 1

Statement by Joe Meade, Irish Data Protection Commissioner at the EEMA (European Electronic Marketing Association) Conference on SPAMMING in Dublin on 3 December 2003.

I am delighted to be present here today to open this very important EEMA conference on SPAMMING. I wish the organisers and participants every success with the Conference and I hope that those of you who are here from Europe, USA and Canada for the first time will have a nice time in Dublin also.

Data Protection Commissioner's role

Data Protection Commissioners do not want to impede responsible businesses doing their work but I expect that business will comply with the relevant regulations and laws. As Ireland's Commissioner I try to operate in a pro business manner but I will always ensure by so doing that a person's right to privacy is fully respected. Also Commissioners are creatures of law-they are not legislators but carry out the duties assigned to them by law- and sometimes their desires or suggestions for effective measures may not be taken on board by legislators who in fairness have to consider all suggestions and all lobby groups.

SPAM

Modern technology has given us the Internet, e-mail, mobile voice communication and SMS text. All are wonderful advances that have revolutionised access to information and provided instant communication. Unfortunately the advantages of speed, ease of use and low cost has also given us the scourge of SPAM. SPAM was not an option in the days of the telegram.

While SPAM is a major cost to Irish and indeed industry worldwide it is above all a major intrusion and invasion of personal privacy. Would industry and governments be so concerned about SPAM and its impact on personal privacy if it was not costing business profit? Its fair to say that most SPAM to business is directed initially to individuals and not primarily to the business. In addition SPAM clogs up personal e-mail accounts to the point where using e-mail from home or from your laptop becomes a burden. The advantage of an email account diminishes when you have to delete hundreds of unwanted messages before you read or send your own mail. The mobile phone is also attacked by unwanted SMS messages. We cannot have a situation where the mobile phone gets bombarded with marketing text messages in the same way that e-mail accounts are and further intrude on our private lives. Indeed this year I have had to take effective action on intrusive SMS messages.

Complaints

Complaints about Marketing have always made up a significant portion of the complaints received by my office each year including 29% of complaints in 2002. A survey I commissioned in late 2002 showed that 50% of people objected to direct marketing by mail while70% had a problem with telephone marketing. Furthermore 56% surveyed now agree that if you use the Internet your privacy is threatened. There was a greater tolerance for electronic marketing methods among younger people but the percentages that objected to this form at 54% are still very high particularly for middle class people and those over 25 years of age. Clearly if these fears are reduced a great business opportunity arises for many. It is not surprising that SPAM and unsolicited text messages are regarded as a nuisance by so many. Direct Marketers have to take these views into account. Annoying the consumer does not make good business sense, respecting their wishes does. Compliance with all of the general data protection principles makes for better customer service and ultimately increases profit.

Let me say that not all marketing by email or SMS is a nuisance if it is done with the required consent. Notice of a special offer from a hotel you stayed in - with prior consent - might be a welcome prompt to do so again.

Irish legislative developments

The announcement in Ireland that the regulations that implement the EU Directive on Privacy and electronic communication - these came into force from 6 November 2003 - will have raised hopes all over the country that the dreaded SPAM is at an end at one stroke. This is not the real position alas. The new regulations with their punitive fines of €3,000 per message will definitely help to combat SPAM but the regulations alone are not the silver bullet that some hope for. I will revert to this in a moment.

The new regulations and fines will I feel in time effectively put an end to most unsolicited e-mail and SMS that originates in Ireland and in the EU. I have the power under the regulations to investigate and prosecute offences related to unsolicited marketing. I will exercise these powers where required and I am confident that my EU colleagues will likewise exercise similar powers in other EU countries.

Irish operations are by and large fairly responsible.

Some will have to strengthen the type of consent they get in order to market by electronic means, in particular where the individuals targeted are not already customers of theirs. Clear opt-in consent will be required. There must be a positive indication by the individual that he/she will accept marketing material from you in an electronic form. Prior to the introduction of these regulations it was possible to send direct marketing material by e-mail if an opt-out was given. This will now only apply where the individual is a customer. To be deemed a customer I will expect that a sale has been made for goods or services or as a minimum the individual has supplied his contact details directly to the business that will do the marketing in connection with a sale. Furthermore at each subsequent mailing the customer's attention should be drawn to the opt-out provisions. While the concept of "similar products and services" can be interpreted restrictively nevertheless I will consider a practical approach to particular areas. Accordingly I will consider whether the marketing meets the reasonable expectations of an individual. If it does not or is clearly an unrelated service or product then a positive opt-in is required

The level of calls received by my office since the new regulations were announced is an indication of the desire of Irish business to comply with the regulations. I am confident that Irish business will quickly comply fully with regulations and to assist them I have put some guidance notes on my website. It should be noted that the Minister is considering the creation of indictable offences and possible prison sentences to further enhance protections for both consumers and business. So business be aware of my new role and adhere to the regulations in full as otherwise you will receive a visit from me.

Why Irish legislation alone is not the solution

So why therefore are the regulations not the silver bullet that some hope for? The problems that we face in tackling this issue are not confined to Ireland or indeed the other EU countries. It is the unsolicited e-mail from outside the EU that is hard to control and this accounts for the greatest percentage of SPAMS. This area has to be addressed urgently.

I note the USA legislation passed last week to curtail SPAM. While it may not be perfect nevertheless a first legal step has been taken in the USA to come to terms with this menace. Hopefully it will have an effect and will over time be improved on. I am also conscious of the legal actions being taken against SPAMMERS by individual companies. As we say in Gaelic "tosach maith leath na hoibre".

In this regard the Minister for Communications Marine and Natural Resources, Dermot Ahern has promised to look for international co-operation, to tackle this problem, during the upcoming Irish EU Presidency. This is a very welcome initiative and one, which I am sure, will be carried forward in future presidencies if necessary, until a successful result is achieved. Furthermore the EU Commission is meeting next week with the national Data Protection Commissioners, the national Communications regulators and the national Consumer Protection Associations in order to discuss issues and have a uniform approach relating to the fight against SPAM in the EU. I also note the actions by the EU Commission at the upcoming Geneva world summit on information society as well as initiatives being taken by OECD, AESM and NAFTA. Lets have action now in a short timeframe and not more talking shops and pleas for action.

What others can do

Individuals themselves and the ISPs can also contribute in their own way. Individuals should be careful when supplying their e-mail address to websites etc. Be conscious of the conditions and the privacy policies and in the time honoured phrase "know and have trust in your customer". In this regard last year the Irish Internet Association in conjunction with my office drew up a standard website privacy policy template for its members to operate so that you as a person would be assured that your personal details were secure.

Effective filtering software from the ISPs and the ability to set up lists of trusted e-mail sources would put the control back in the hands of the individual. Blocking certain addresses or keywords can be effective also and I appreciate the efforts being made by the industry to enhance these tools.I may well need the assistance of the ISPs in following up on complaints and I am confident that this co-operation will be forthcoming as it has been to date.

Let me also acknowledge the contribution Industry overall is making already but more is needed.

A shared responsibility

Clearly the industry itself - be it the IT industry, corporations or commercial marketing companies- along with regulators and governments worldwide will have to take appropriate actions, as otherwise SPAM will destroy the industry because where personal privacy is being increasingly intruded on a majority of people may stop using it to a degree. Accordingly we all have a shared responsibility and we have to achieve international cooperation to address this problem. Laws alone will not solve it unless every country buys into it and appropriate sanctions are implemented effectively and industry wholeheartly wants success.

At the end of the day people, business and indeed Data Protection Commissioners do not want to be annoyed and the more a person gets annoyed the less profit you will make.

The broader context

Data Protection is not solely about SPAM and in that regard the principles for protecting personal data - fairness, accuracy, purpose, sufficiency, time, transparency, security and proportionality - must be adhered to by all and sundry no matter how data is collected. I ask industry in particular but also governments worldwide to:

- balance all interests in a proportionate manner
- carry out privacy impact statements before any systems are developed
- constantly review your operations
- to avoid having Privacy Invasive Technology but to install Privacy Enhancing Technology.

As you all appreciate data protection is not a hindrance to commerce or government but in fact the key enabler.

I trust that the conference that I now formally open will be a successful, inspiring and problem solving one.

Appendix 2

Publication of Freedom of Information requests on State bodies websites

From April 2003, the Department of Communications, Marine and Natural Resources (CM&NR) commenced publishing details of FOI requests it had received on its website, with the exception of requests for personal information. The information initially displayed comprised the name and address of the requester and a synopsis of the information sought.

I took the view that, under Data Protection legislation, publication of personal data relating to individuals making Freedom of Information requests in their personal capacity cannot be legitimately published as this is not a legislative requirement for making a Freedom of Information request. I accepted that personal data relating to persons making such requests in a professional or business capacity could be published.

When my view was not accepted, I issued an Enforcement Notice to the Department of CM&NR in October 2003 requesting that the practice cease. The notice was appealed but following subsequent agreement between myself and the Attorney General- this was acceptable to the Minister for CM&NR- which lead to my withdrawing the Enforcement Notice, the Department modified its practice to the extent that the details of private citizens (as opposed to individuals making requests in a professional or business capacity) will no longer be published.

I set out now the text of the agreement between myself and the Department of CM&NR which should be used by all bodies subject to Freedom of Information legislation in order to ensure compliance with the Data Protection Acts 1988 and 2003.

Agreement: Minister for CM&NR -v- Data Protection Commissioner

1. Where a member of the public makes an FOI request to the Department for personal information whether relating to that person or to another, no details of the requester or the records requested shall be posted on the Department's FOI website.

2. Where a person who states himself/herself to be a journalist or whom the Department knows or has good reason to believe is a journalist makes an FOI request to the Department, and it appears to the Department that the records have been requested for use in the journalist's professional capacity, details of the name, address and profession of the requester, and details of the records requested, may be posted on the Department's FOI website.

3. Where a person stating himself/herself to act on behalf of a solicitor or whom the Department knows or has good reason to believe is a solicitor, makes an FOI request to the Department and it appears to the Department that the records have been requested for use in the solicitor's professional capacity, details of the name, address and profession of the requester and of the records requested may be placed on the Department's FOI website.

4. Where a person stating himself/herself to act on behalf of a company, firm or other business, or whom the Department knows or has good reason to believe is acting on behalf of a company firm or other business, makes an FOI request to the Department, and it appears to the Department that the records have been requested for use by the requester for business purposes, details of the name address and business or firm of the requester, and of the records requested, may be posted on the Department's FOI website.

5. Where the Department cannot ascertain the status or profession of an FOI requester, or where it is uncertain as to whether the records requested are to be used in a professional or business capacity, then if in the opinion of the Department there is a real risk that posting details of the request and requester on its FOI website would result in the disclosure of an individuals personal information to the public, the request shall be dealt with as a request for personal information under paragraph 1 above.

6. Where records are to be posted on the Department's website the Department shall continue the practice of redacting information that is personal or confidential.

In January 2004 I wrote to all Secretary Generals and Heads of other Offices requesting that Departments and offices under their aegis bear in mind the basis on which the Enforcement Notice against the Minister for CM&NR was lifted in the event that it is decided to place FOI requests on a website. As a general principle, staff should bear in mind that the publication of personal data, such as the name and address of a person making an FOI request (as distinct from a requester acting in a professional or business capacity), constitutes a disclosure under the Data Protection Acts 1988 and 2003.

Appendix 3

Vetting of persons for employment purposes

Right of access

As a living individual everybody has the right to obtain a copy of all personal data relating to them by making a written "access request" to any organisation or individual who holds personal information about them. This right of access covers both "manual data" and "automated data".

The "right of access" - which is the key aid provided by section 4 of the Data Protection Acts to assist a data subject in defending his privacy interests - should not be used in a manner which brings about the disclosure to third parties of information which might not otherwise be available to them. That is why the Data Protection (Amendment) Act 2003 has a provision included to prevent employers forcing data subjects to allow them to access their personal data held by the Gardaí in particular or by any other organisation i.e. "enforced subject access". This provision has not been implemented pending the setting up by the Gardaí of a national clearance system.

What is enforced subject access?

While any person is entitled to ask for information, the question arises as to whether a data controller is obliged to make the data available or has discretion in the matter. Where an access request is made under section 4 the data controller has no discretion. In such cases the data must only be given to the data subject concerned and not to a third party. What data subjects do with their personal data is entirely a matter for them.

What I term "enforced subject access" under Section 4 has consequences which go way beyond access by employers to details of criminal convictions kept by An Garda Síochána. For example, enforced subject access, if left unchecked, raises the issue of access by other third parties e.g. landlords, insurance companies or sporting organisations requiring applicants for housing, insurance cover or club membership to access their data in respect of bank records, medical records, DNA databases, etc. as a prerequisite to acceptance of their application. It is for this reason that it appears to me, as a matter of public policy, that it is as important that the practice of enforced subject access be outlawed as it is to ensure the controlled availability of details of a person's previous criminal convictions for particular purposes. This provision of the Act should be implemented as early as possible following the establishment of suitable vetting systems by the Gardaí.

Data may be released by a data controller to a third party under section 8(h) which provides that the restrictions on disclosure of personal data provided for in the Acts do not apply in circumstances where the data subject has given consent. Where a data subject has given such consent, the data controller has discretion in the matter as there is no obligation on him or her to accede to the request - the data controller should be guided by proportionality having regard to the circumstances. Should a data controller decide to make the data available, he or she may rely on section 8(h). In employment terms this could amount to "enforced subject access" if appropriate regard is not had to proportionality as the person may have little option but to agree to the employer's wishes.

Vetting service

The system of personal subject access requests under section 4 of the Act needs to be distinguished from the vetting service currently provided by An Garda Síochána for prospective employees in a number of areas including child access, Government employees, State contractors and adoption applicants. An Garda Síochána has established a Central Vetting Unit for responding to the latter requests with the written consent of the individual concerned.

Spent convictions

Irish legislation makes no provision for "spent convictions" and the indefinite retention of minor convictions does not accord with the spirit of data protection legislation regarding retention for as long as is necessary for the purpose for which it was obtained. The March 2002 National Economic and Social Forum Report No. 23 recommended that equality legislation be expanded to include the right to be protected from discrimination on the grounds of criminal conviction. In my observations to the Department of Justice Equality and Law Reform on this Report, I pointed out that section 2(1)(c)(iv) of the Data Protection Act provides that personal data held on computer "shall not be kept for longer than is necessary for (the) purpose". In the light of this, I expressed the view that there should be legislative provision for "spent convictions" after a reasonable period in respect of minor offences which, on any

reasonable view, would not be relevant to an assessment by An Garda Síochána of whether a person leads or has led a law-abiding life. Until such time as legislation along these lines is enacted, it is reasonable that employers should only take relevant offences into account and make fair judgments. I should point out that, although such data may be fairly obtained by employers under current legislation, the manner in which an employer processes data is subject to the provisions of the Acts. As such, if the processing is not conducted in compliance with legislation, I may be obliged to take enforcement action against such an employer. Furthermore, should an individual be harmed by the manner in which an employer processes his/her data, that individual has a right to seek civil remedy under section 7 of the Acts.

What data should be provided?

In my discussions with An Garda Síochána, I suggested - in the light of the provision in the Act that data "shall not be kept for longer than is necessary for (the) purpose" and the current situation concerning 'spent convictions' - that it would be appropriate for An Garda Síochána to provide information of relevance to the prospective employer. Obviously if someone has a conviction relating to child sexual abuse, that information is of primary significance to an employer in the childcare sector or in other areas where access to children arises. Conversely, information about an individual's payment of a fine for perhaps bicycling offences in his youth, or perhaps speeding offences, would not be relevant, and it may be inappropriate for An Garda Síochána to choose to provide this information in response to a vetting request. However, An Garda Síochána stated that their policy in responding to vetting requests from prospective employers follows guidelines established as a result of advices from the Office of the Attorney General. These advices stipulate that when An Garda Síochána is asked a "convictions/no convictions" question, they are obliged to return convictions recorded where applicable. The Gardaí feel it had not been envisaged that they would be obliged to make a decision on what convictions should be notified to a prospective employer and what ones should not. This area needs to be reviewed.

Should all employments be subject to Gardaí vetting procedures?

It would be disproportionate to introduce a police vetting facility in respect of all employment sectors. A vetting system should not be used as a form of State-endorsed character reference. Its function is to identify individuals who are unsuited to certain types of employment by virtue of a real or perceived risk that they might present. Therefore, it would seem appropriate for An Garda Síochána, when exercising its discretion under section 8 of the Data Protection Acts in responding to vetting requests, to consider only requests from sectors for which vetting information is relevant and desirable from a crime prevention viewpoint: such as the area of access to children, and perhaps other sectors such as the private security industry or the award of public vehicle licences, as considered appropriate. Providing a vetting service on a general basis would be disproportionate and would appear to intrude unduly into the privacy of individuals, particularly when it is borne in mind that jobseekers, when agreeing to vetting searches being carried out by their prospective employers, may be subject to limitations upon their freedom of action and freedom to withhold consent. Ultimately this is a matter for the Oireachtas.

What to withhold?

An Garda Síochána may have a range of details recorded in respect of particular individuals. When responding to vetting requests, it is appropriate for An Garda Síochána to provide information of relevance to the prospective employer. It would therefore be appropriate for An Garda Síochána to devise and implement a policy regarding the nature of details that would be provided in response to vetting requests, and the nature of information that it is more appropriate to withhold. As indicated above discretion should be given to the Gardaí with suitable legislative provisions.

Soft intelligence

The question of "soft intelligence" being provided has also been raised as well as the length of time data should be kept by the Gardaí. I feel that whatever police forces consider being of operational assistance - and which could be so justified to a member of the judiciary if necessary - can be retained

for as long as they deem it appropriate. Whether this information should be disclosed, particularly for sensitive job applicants, is a matter not alone for the Gardaí but ultimately for legislation by the Oireachtas. However a proper balance has to be struck because disclosure of "soft intelligence" can unintentionally cause more damage to a person than was ever envisaged when it was properly retained solely as an aid to Garda operational matters.

Retention of vetting requests data

The fact that an intelligence purpose may be served by retaining records of vetting requests in respect of certain individuals would not, in itself, justify a general policy of indefinite retention of such records in respect of all individuals. In my view, An Garda Síochána and police forces in general might legitimately decide not to delete certain records in particular cases where there was a clear intelligence benefit to retaining such records. These particular cases might need to be certified or authorised by a Garda member of suitably senior rank such as Chief Superintendent (which is the rank specified in section 8(b) of the Act in a broadly analogous context). However, it would not be appropriate, in my view, routinely to retain all such data, in respect of all individuals, indefinitely.

In cases where An Garda Síochána consider it appropriate to retain records of vetting requests for intelligence purposes, then the appropriate retention period would be related to the usefulness and relevance of those records for intelligence purposes. The retention period would be "indefinite" in the sense that the period of usefulness and relevance of the data would not be known from the outset.

Future

Clearly this whole area needs to be examined in detail with special safeguards established in stand alone legislation along with a suitable period for public consultation. In this regard the code of practice on data protection being developed by the Gardaí will be a useful document as it will detail what information can be supplied by the Gardaí under the Data Protection Acts.

Appendix 4

Statement at the Biometrics Forum in Dublin by Joe Meade Irish Data Protection Commissioner on 24 July 2003.

I welcome this forum.

What are biometrics?

The term "biometrics" is taken to mean the identification of individuals based on a physical characteristic using information technology. A physical characteristic, such as the fingerprint, is digitalised by the biometric system and then depicted either as a biometric image or as a biometric template. A template is a biometric number calculated from certain unique characteristics in the fingerprint. Because the other information contained in the image is not used in the calculation of the template, it is not possible to retrospectively regenerate the original image of the fingerprint from the biometric template.

General data protection issues

I will now make some general comments about Data Protection before I go on to the topic of Biometrics and European data protection views. Improved levels of service, identification, antifraud measures, surveillance actions to prevent and investigate crime - including cyber crime - and terrorism are put forward as necessary in the modern global world. While we all can accept the need for many of these initiatives there is, however, a real danger that the human right to privacy can be overlooked or indeed diminished by some of these demands if a proper balance is not struck. Accordingly, if we are being asked to sacrifice our privacy rights we must have details about what we get in return. Once privacy rights are surrendered they may be hard to recover. We should therefore surrender these rights reluctantly, on the basis of convincing arguments and facts about other interests of society which need to be balanced. Legislators and business, accordingly, have a responsibility to debate these matters in an open and frank manner. Today's forum is therefore a positive event.

I believe it appropriate to reiterate that as Data Protection Commissioner I am also conscious of the sensitive issues of crime and security, including national security. As Data Protection Commissioner, I will be supportive of measures that are demonstrably necessary to protect against crime or terrorism but such measures must be proportionate and have regard to the human right to privacy.

Biometrics and data protection

As regards Biometrics, Ann Cavoukin - Ontario's Privacy and Information Commissioner - has just now clearly outlined to you all the concerns that can be there for ordinary folk, the positive role of a data protection commissioner, the dangers that can arise if systems are not developed properly while also recognising the benefits and industries role.

As a national DPC let me say that I and indeed my European and world-wide colleagues are not against Biometrics and we hope that industry recognises our positive role in that regard. At the end of the day as Data Protection Commissioner I am a creature of law charged with ensuring that a fundamental human right to privacy for the individual is respected. That does not mean that DPCs are luddites and are not in favour of IT developments to improve operations, to administer efficiently and to improve verifications. As I said in my general remarks the balance has to be proportionate to your right to personal privacy.

Data Protection Commissioners' views

In Ireland I see many benefits in Biometrics but there is also a need for constructive dialogue between the industry and national and European DPCs to get the balance right. This dialogue has to be open on both sides. At European level the Article 29 Working Party (see below for current position) is bringing out a working document in this area soon and we see it as the start of a dialogue which should eventually lead to a code of practice. I ask the industry to partake in the dialogue and to start drawing up such a code but the industry has to accept that in the EU, member states have somewhat differing legal systems and different cultures. The challenge in drawing up a code or in industry operations is to respect those differences though that should not be a major obstacle given the intellectual capability of the industry personnel The Eurodac system has recognised the importance of data protection in that it is subject to supervision by national and EU commissioners. The same applies to the Schengen system.

What the public demand

As with any IT system we should not rely on DPC or legislation alone to protect a human right. Let the industry develop privacy enhancing technologies and other IT solutions so that privacy is seen as a competitive advantage and not in a negative light or as a hindrance. I say that because in a survey I carried out last year personal privacy rated after crime prevention as the major concern of people while 75% surveyed felt that business are encroaching on personal privacy. Though 54% felt they can trust business to use personal information about them in a fair and proper manner nevertheless 25% actively disagreed with that statement. Therefore there is a challenge and an opportunity for all here to consider and indeed improve on these findings. Finally DP is the key enabler of eCommerce, eGovernment, security and indeed biometric systems while empowering a person to protect his/her right to privacy. Therefore the more privacy compliant and transparent systems are the better for everyone. Accordingly I look forward at national and European level to positive progress being achieved in this complex and ever-changing environment.

As a final thought I ask you to reflect on the following-as a person are you happy that the system being developed by you or your organisation gives you adequate privacy protection? If not do something about it as there is a problem otherwise. We should test ourselves for satisfaction.

Post statement developments

(a) Article 29 Working document

The working document issued on 1 August 2003 in its conclusions opined that:

- The Working Party is of the view that most biometric data imply the processing of personal data. It is therefore necessary to fully respect the data protection principles provided for in Directive 95/46/EC taking into account the particular nature of biometrics inter alia the ability to collect biometric data without the knowledge of the data subject and the quasi certainty of the link with the individual, when developing biometric systems.
- A respect for the principle of proportionality which forms the core of the protection ensured by Directive 95/46/EC imposes, especially in the context of authentication/verification, a clear preference towards biometric applications that do not process data obtained from the physical traces unknowingly left by individuals or that are not kept in a centralised system. This allows the data subject to exercise better control on the personal data processed about him or her.
- The Working Party intends to revisit this working document in the light of the experience of data protection authorities and technological developments linked to biometric applications. As biometric data is even at the present time being introduced for a wide range of uses in a number of different forums, future work will be necessary without delay especially in the context of employment, visa and immigration and travel security.
- While the responsibility remains to be on the industry to develop biometric systems that are data protection compliant, a working dialogue, in particular on the basis of a draft code of conduct, between all interested parties including data protection authorities would be a great benefit from all perspectives.)

(b) Central storage of biometrics

The Article 29 Working Party also noted that in principle it is not necessary for the purposes of authentication/verification (establishing that the person is the same person as expected, i.e. a - 1:1 check) to store the biometric template in a centralised database. On the other hand, the process of identification (establishing precisely who someone is, i.e. a 1: many check) can only be achieved by storing the biometric data in a centralised database, because the system, in order to identify the data subject, must compare his/her template with the template of all persons whose data are already centrally stored. I endorse the distinction between authentication/verification and identification as crucial. In most situations, it is sufficient to verify who the person is. Identification and central storage, therefore, should not be used when authentication/verification applications are sufficient. This is central to the principle of proportionality in Data Protection Law.

Appendix 5

Genetic Data - views of Data Protection Commissioners of the EU (Article 29 Working Party) in a working document adopted by them in March 2004

Given the fast moving age of technological, scientific and economic developments in the field of genetics and taking into account the variety of purposes for which the processing of genetic data may take place, the Working Party felt it was necessary at this stage to define a common approach with a view to establishing the appropriate safeguards for the processing of genetic data. The main lines of this approach can be summarised as follows:

- Any use of genetic data for purposes other than directly safeguarding the data subject's health and pursuing scientific research should require national rules to be implemented, in accordance with the data protection principles provided for in the Directive, and in particular the finality and proportionality principles. The application of these principles renders the blanket implementation of mass genetic screening unlawful.

  Furthermore, in accordance with these principles, the processing of genetic data should be authorised in the employment and insurance fields only in very exceptional cases provided for by law, so as to protect individuals from being discriminated against on the basis of their genetic profile.

  In addition, the ease with which genetic material can be obtained unbeknownst to the data subject and the relevant information can be subsequently extracted from such material, requires strict regulations in order to prevent the dangers related to new forms of "identity theft" - which would be especially dangerous in this sector and might affect fatherhood and motherhood, or even the possibility of using the material for cloning purposes. This is why, in regulating genetic data, one should not fail to consider the legal status of the DNA samples used for obtaining the information at stake. Among the issues addressed, special importance should be attached to the application of a wide range of data subjects' rights to the management of such samples, as well as to destruction and/or anonymisation of the samples after obtaining the required information.

  Finally, procedures should be put in place in order to ensure that genetic data are only processed under the supervision of qualified professionals who are entitled to such processing on the basis of specific authorisations and rules.

- In Member States where the purposes and the appropriate safeguards for the processing of genetic data are not established by law, the DPAs are encouraged to play an even more active role in ensuring that the finality and proportionality principles of the Directive are fully respected.

  In this respect, the Working Party recommends that Member States should consider submitting the processing of genetic data to prior checking by DPAs, in accordance with Article 20 of the Directive. This should in particular be the case with regard to the setting up and use of bio banks.

  Moreover, closer cooperation and exchange of best practices between DPAs could prove to be an efficient way to compensate the present absence of regulatory framework in the field of the on-line "genetic testing direct to the public".

- It is worth noting that a new, legally relevant social group is coming into existence - namely, the biological group, the group of kindred as opposed, technically speaking, to one's family. Indeed, such a group does not only include family members such as one's spouse or foster children, but it can also consist of entities outside this family circle - whether in law or factually (e.g. gamete donors).

The Working Party intends to revisit this working document in the light of the experience acquired by the data protection authorities with regard to the processing of genetic data. This document should be regarded as a stepping stone towards further discussions on the issues at stake. The Working Party will closely monitor the evolution of said issues and may decide to focus in detail on specific areas at a later stage, in order to keep in line with the technological developments linked to the processing of genetic data.

Appendix 6

Presentations and talks (70 overall) given by the Data Protection Commissioner and staff in 2003.

Organisation	Date	DPC Official
UCC Department of Law	*8 December*	*Joe Meade*
IBEC Limerick	*5 December*	*Joe Meade*
EEMA Spam Conference Dublin	*3 December*	*Joe Meade*
Department Enterprise Trade and Employment	*2 December*	*Nelius Lynch*
Waterford County Council	*1 December*	*Aileen Harrington*
Letterkenny IT	*27 November*	*Sean Sweeney*
Dublin Institute of Technology	*18 November*	*Nelius Lynch*
DIT, Cathal Brugha St. Dublin	*19 November*	*Aileen Harrington*
Institute of Public Administration	*19 November*	*Seán Sweeney*
Galway County Council	*12 November*	*Aileen Harrington*
ESB Data Protection Review Group	*12 November*	*Joe Meade & Anne Gardner*
Arthur Cox Solicitors	*11 November*	*Joe Meade*
Quantum Health, Carlow	*1 November,*	*Tom Maguire*
Jurys Doyle Hotels	*30 October*	*Aileen Harrington*
Employment Conference, Dublin	*29 October*	*Joe Meade &Tom Maguire*
Dublin- General DP Conference	24 September	Joe Meade
Ombudsman / Information Commissioner's Office	*23 October*	*Tom Maguire*
South Western Area Health Board	*10 October*	*Nelius Lynch*
Workshop for Department of Justice E & LR Agencies	*9 October*	*Tom Maguire*
Health Boards DP Training	*8 October*	*Tom Maguire*
Cyprus Conference	*8 October*	*Joe Meade*
Law Society of Ireland, Thurles	*3 October*	*Joe Meade*
Kilroys Solicitors, Dublin	*2 October*	*Joe Meade*
Western Health Board, Galway	*1 October*	*Tom Maguire*
Irish Internet Association Annual Conference	*29 September*	*Joe Meade*
Irish Computer Society Fellows Lunch	*25 September*	*Joe Meade*
University College Dublin	*22 September*	*Nelius Lynch*
Comhairle	*18 September*	*Aileen Harrington*
Info Ireland 2003	*18 September*	*Aileen Harrington*
25th International Conference Sydney	*11 September*	*Joe Meade*
The National Concert Hall	*10 September*	*Aileen Harrington*
BINOCAR, TCD	*8 September*	*Sean Sweeney*
Freedom of Information Conference Berlin	*1 September*	*Joe Meade*
Local Authorities, Limerick	*26 August*	*Tom Maguire*
Irish Red Cross	*13 August*	*Aileen Harrington*
Department of Community, Rural and Gaeltacht Affairs	*12 August*	*Aileen Harrington*
Health Board DP Training	*11 August*	*Nelius Lynch*
Jury's Hotels, HR Managers	*6 August*	*Aileen Harrington*
European Biometrics Forum Dublin	*24 July*	*Joe Meade*

National Childcare Co-ordinating Committee (NCCC)	*23 July*	*Anne Gardner*
Irish Bankers Federation	*17 July*	*Joe Meade*
IBEC-technology group-Dublin	17 July	Joe Meade
Departments and State Offices	*9 July*	*Tom Maguire*
University College Dublin	*1 July*	*Tom Maguire*
E-Security Seminar Wexford	1 July	Nelius Lynch
Survive Forum (Security)	26 June	Tom Maguire
Departments and State Offices	*24 June*	*Joe Meade & Tom Maguire*
St. James's Hospital	*19 June*	*Tom Maguire*
Institute of European Affairs	*17 June*	*Joe Meade*
IBEC Employment Seminar, Dublin	*11 June*	*Sean Sweeney*
Health Boards DP Liaison Officers Workshop,Limerick.	*9 June*	*Tom Maguire*
Garda Chief Supts. Training, Templemore	*6 June*	*Joe Meade*
National Payroll Conference Dublin	*27 May*	*Tom Maguire*
National Childminding Association of Ireland	*15 May*	*Anne Gardner*
Ernest and Young Cork	*2 May*	*Joe Meade*
IDMA Annual Conference	*29 April*	*Joe Meade*
Recruitment Federation Conference Dublin	*29 April*	*Tom Maguire*
McCann Fitzgerald Solicitors	*10 April*	*Joe Meade*
Arthur Cox Solicitors	*11 April*	*Joe Meade*
Health Boards FOI Networks Meeting	*9 April*	*Tom Maguire*
European DP Commissioners Conference, Seville	*4 April*	*Joe Meade*
Freedom of Information Conference, Tullamore	*19 March*	*Tom Maguire*
ISACA Conference Dublin	*7 March*	*Joe Meade*
NIETS Conference Dublin	*27 February*	*Joe Meade*
Justice Equality and Law Reform Retention of Traffic Data Forum	*24 February*	*Joe Meade*
Garda Chief Supts Training, Templemore	*19 February*	*Joe Meade & Tom Maguire*
Health Regulatory Bodies	*17 February*	*Tom Maguire*
Trinity College, Health Informatics	*1 February*	*Tom Maguire*
Justice, Equality, Defence and Women's Rights, Oireachtas Committee	*23 January*	*Joe Meade*
Eastern Region Health Authority	*14 January*	*Joe Meade & Tom Maguire*

Joe Meade Commissioner; Tom Maguire Deputy Commissioner; Nelius Lynch, Aileen Harrington and Anne Gardner Assistant Commissioners; Sean Sweeney, Senior Compliance Officer.

In addition to the foregoing many other staff gave in house presentations as part of the overall staff development and training programme.

Appendix 7

Office of the Data Protection Commissioner Receipts and Payments in the year ended 31 December, 2003

2002 €		2003 €
	Receipts	
750,173	Moneys provided by the Oireachtas (Note 1)	1,132,733
358,067	Fees (Note 2)	455,539
1,108,240		**1,588,272**
	Payments	
547,239	Salaries & Allowances (Note 3)	694,049
35,078	Travel & Subsistence	36,378
10,275	Office & Computer Equipment	43,418
646	Furniture & Fittings	131,593
13,404	Equipment Maintenance & Office Supplies	48,810
11,491	Accommodation Costs (Note 4)	26,904
19,632	Communication Costs	39,968
44,448	Incidental & Miscellaneous	13,586
58,912	Education & Awareness	49,920
9,048	Legal & Professional Fees	48,107
750,173		**1,132,733**
358,067	Payment of fees to Vote for the Office of the Minister for Justice, Equality & Law Reform	455,539
1,108,240		**1,588,272**

Notes

1 Moneys provided by the Oireachtas The Commissioner does not operate an independent accounting function. All expenses of the Office are met from subhead F of the Vote for the Office of the Minister for Justice, Equality and Law Reform. The expenditure figures in this financial statement detail the payments made by the Department of Justice, Equality and Law Reform on behalf of the Office.

2 Fees Fees paid to the Data Protection Commissioner in respect of registration and enquiries are transferred intact to the Vote for the Office of the Minister for Justice, Equality and Law Reform as appropriations-in-aid.

3 Salaries, allowances and superannuation (a) The Commissioner is appointed by the Government for terms not exceeding five years and his remuneration and allowances are at rates determined by the Minister for Justice, Equality and Law Reform with the consent of the Minister for Finance, (b) Staff of the Commissioner's Office are established civil servants. Their superannuation entitlements are governed by the Regulations applying to such officers. A superannuation scheme for the Commissioner as envisaged in the Act was adopted by Statutory Instrument No.141 of 1993.

4 Premises The Office of Public Works provides the premises at the Irish Life Centre, Abbey Street, Dublin 1, to the Commissioner without charge. The cost borne by the Office of Public Works for this accommodation in 2003 was €70,000 (€63,497 in 2002).

Appendix 8

Registrations 2001 / 2002 / 2003

		2001	2002	2003
(a)	**public authorities and other bodies and persons referred to in the Third Schedule**			
	Civil service Departments/Offices	113	116	**118**
	Local Authorities & VECs	118	139	**138**
	Health Boards/Public Hospitals	56	57	**59**
	Commercial State Sponsored Bodies	53	43	**45**
	Non-Commercial & Regulatory	139	164	**171**
	Third level	40	45	**54**
	Sub-total	519	564	**585**
(b)	**financial institutions, insurance & assurance organisations, persons whose business consists wholly or mainly in direct marketing, providing credit references or collecting debts.**			
	Associated Banks	35	42	**46**
	Non-Associated Banks	60	58	**62**
	Building Societies	6	6	**6**
	Insurance & related services	164	182	**230**
	Credit Union & Friendly Societies	442	447	**449**
	Credit Reference/Debt Collection	22	22	**28**
	Direct Marketing	57	64	**61**
	Sub-total	786	821	**882**
(c)	**any other data controller who keeps sensitive personal data**			
	Primary & Secondary Schools	26	33	**340**
	Miscellaneous Commercial	53	79	**77**
	Private Hospitals/Health	99	107	**125**
	Doctors, Dentists, Health Professionals	425	467	**576**
	Pharmacists	643	667	**828**
	Political parties & public representatives	90	95	**108**
	Religious, voluntary & cultural organisations	57	91	**118**
	Legal Profession	4	93	**445**
	Sub-total	1,398	1,632	**2,617**
(d)	**those required under S.I. 2/2001**			
	Telecommunications/Internet	7	3	**10**
(e)	**data processors**	390	412	**524**
	TOTAL	3,099	3,632	**4,618**

Data Protection
Commissioner
An Coimisinéir Cosanta Sonraí

Data Protection Commissioner
Block 6
Irish Life Centre
Lr Abbey Street
Dublin 1
Tel. (01) 874 8544 Fax. (01) 874 5405
eMail. info@dataprotection.ie
Web. www.dataprotection.ie

Coimisinéir Cosanta Sonraí
Bloc 6
An t-Áras Árachais
Sráid na Mainistreach Íochtarach
Baile Átha Cliath 1
Tel. (01) 874 8544 Fax. (01) 874 5405
eMail. info@dataprotection.ie
Web. www.dataprotection.ie